AVERTISSEMENT

LIENS

Code la Propriété Intellectuelle – Articles L. 122-4 et L. 335-1 à L. 335-10
Loi n°92-597 du 1er juillet 1992, publiée au *Journal Officiel* du 2 juillet 1992
http://www.cfcopies.com/V2/leg/leg-droi.php
http://www.culture.gouv.fr/culture/infos-pratiques/droits/protection.htm

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITE DE TOULOUSE

Délivré par l'Université Toulouse Capitole

École doctorale :**Sciences Juridiques et Politiques**

Présentée et soutenue par

LACOSTE-VAYSSE Guillaume

le 25 novembre 2016

La protection des données de santé à caractère personnel
Pour la reconnaissance des droits du patient

Discipline : **Droit**

Spécialité : **Droit Privé et Sciences Criminelles**

Unité de recherche : **IDP (EA 1920)**

Directeur de thèse : Monsieur Jean DEVEZE, Professeur des universités, Université Toulouse Capitole I.

JURY

Monsieur Jean FRAYSSINET, Professeur émérite, Aix-Marseille Université.
Madame Nathalie MALLET-POUJOL, Directrice de Recherche au CNRS, UMR 5815, Université de Montpellier.
Madame Corinne MASCALA, Professeur des universités, Université Toulouse Capitole I.

La protection des données de santé à caractère personnel.

Pour la reconnaissance des droits du patient.

« L'université n'entend ni approuver ni désapprouver les opinions particulières du candidat ».

REMERCIEMENTS

Je tiens à remercier tous ceux qui m'ont soutenu durant la rédaction de cette thèse.

Tout d'abord je tiens à adresser toute ma gratitude et ma reconnaissance à Monsieur le Professeur J. Deveze qui m'a accordé toute sa confiance ainsi que son soutien.

Je souhaite également remercier Madame la présidente C. Mascala pour sa confiance et pour avoir accepté d'évaluer mes travaux.

Je tiens à remercier Madame la Directrice N. Mallet-Poujol et Monsieur le Professeur J. Frayssinet d'avoir accepté d'évaluer mes travaux et de me faire l'honneur de leur présence.

Je remercie Madame M-F Ille, secrétaire de l'école doctorale, pour sa présence bienveillante et sa disponibilité.

Je tiens également à remercier J-P. Charrière qui m'a apporté énormément de soutien et qui a su me redonner confiance.

A mon frère Jean-Marc qui ne m'a jamais oublié, m'a soutenu et « secoué » par moment.

A ma compagne Clémence qui m'a accompagné à chaque instant, et qui a su être disponible pour m'aider dans mon travail.

A mes deux plus fidèles amis, Guillaume et Antonin.

A toute ma famille et mes parents, Christine et Guy, qui n'ont jamais cessé de croire en moi et qui sont mes exemples.

Liste des principales abréviations :

ANSSI Agence nationale de la sécurité des systèmes d'information

ASIP Santé Agence des Systèmes d'Information Partagées de Santé

CAH Comité d'Agrément Hébergeur

CIL Correspondant Informatique et Libertés

CNIL Commission Nationale de l'Informatique et des Libertés

CNOM Conseil National de l'Ordre des Médecins

COFRAC Comité Français d'Accréditation

CSP Code de la Santé Publique

DMP Dossier Médical Personnel

DPD Délégué à la Protection des Données

G29 Groupe de travail de l'article 29

GAFA Google/Apple/Facebook/Amazon

GIP Groupement d'Intérêt Public

HAS Haute Autorité de Santé

HON « Health On the Net » traduit par « santé sur l'internet »

INS Identifiant National de Santé

INS-C Identifiant National de Santé Calculé

LCEN Loi pour la Confiance dans l'Economie numérique

LIBE (commission) Libertés civile, justice et affaires intérieures

LIL Loi Informatique et Libertés

LRN Loi pour République Numérique

NIR Numéro d'Inscription au Répertoire

NTIC Nouvelles Technologies de l'Information et de la Communication

RGS Référentiels Généraux de Sécurité

TFUE Traité de Fonctionnement de l'Union Européenne

TIC Technologie de l'Information et de Communication

Sommaire

Introduction

« Si vous torturez suffisamment de données, la nature se révélera toujours [1]»

-Ronald Coase-

1. L'information à travers l'histoire : illustration.- La connaissance de l'Homme et de son Histoire a été reconstituée grâce aux recherches de scientifiques et historiens. En effet, c'est avec le recoupement des traces et des vestiges[2] laissés par les hommes, tout au long de leur existence, que les anthropologues et ethnologues ont pu mettre en lumière l'évolution de l'humanité et des comportements grâce à l'étude des différents modes de vie des êtres humains. Ces recherches avaient notamment pour objectifs de *décrypter* et interpréter les informations laissées par nos ancêtres. En d'autres termes, l'Homme a « marqué » les événements de son existence. Par exemple, des peintures pariétales ont permis de reconstituer un mode de vie des hommes à l'ère paléolithique. Ces informations laissées par l'Homme lui permettaient, non seulement de *fixer* une histoire dans le temps, mais aussi de communiquer et transmettre un savoir ou un événement. C'est à travers l'étude des écritures cunéiformes, des hiéroglyphes, des calligraphies, des idéogrammes et des alphabets divers que nous avons constaté que l'Homme avait toujours utilisé des moyens de *représentation* de l'information.

2. Outre les moyens de représentation de l'information, le support de stockage a, lui aussi, évolué avec le temps. En effet, nous sommes passés de l'argile, la pierre, le bois, le cuir, le métal et le parchemin au silicium et à la miniaturisation des supports, avec, par exemple, les cartes à puce et les clés *Universal Serial Bus* (USB). Les capacités de dématérialisation ont permis de mettre en place des solutions de stockage virtuel telles que le « cloud computing » dont la traduction littérale « *stockage en nuage* » tend à faire croire que ces nouveaux modes de stockage sont éphémères ou *insaisissables.* Le « cloud computing » est, à l'origine, une expression issue de l'habitude des concepteurs de réseaux.

---

[1] Traduction de l'anglais « *If you torture data enough, nature will always confess ». in* : Gordon Tullock, "A Comment on Daniel Klein's 'A Plea to Economists Who Favor Liberty'", *Eastern Economic Journal*, Spring 2001.

[2] B. Galinon-Méménec, S. Zlitni, F. Liénard, « L'Homme-trace, Inscriptions corporelles et techniques », Coll. CNRS Alpha, 30 décembre 2015.

En effet, lors des premiers usages d'internet, les concepteurs schématisaient les réseaux sous la forme de nuage[3]. La forme actuelle du stockage en « nuage » est une forme abstraite d'une infrastructure informatique, c'est-à-dire que le cloud computing rassemble à la fois les serveurs, les applications, les données et, enfin, les plateformes. On relève trois caractéristiques essentielles du fonctionnement du stockage en nuage. La première est le fait que le service de stockage permet un accès et une gestion immédiate des informations par l'utilisateur. La seconde caractéristique est l'assurance d'un accès instantané et d'une excellente rapidité de connexion. Cette hyper connectivité est assurée par un accès à toutes les bandes du réseau, c'est-à-dire que tous les fournisseurs de réseaux offrent une bande passante[4] de connexion sur la totalité de la planète. Cet accès permet ainsi de se connecter au système virtuel de stockage en moins de 50 millisecondes[5]. Enfin, la troisième caractéristique est la non-localisation des ressources. C'est-à-dire que l'organisation du stockage en nuage permet la mise à disposition de milliers de serveurs autorisant ainsi une augmentation rapide de la capacité de stockage. Cette *absence* de localisation des serveurs permet de stocker les informations dans la zone géographique la plus proche de l'utilisateur. Cependant, l'absence de « localisation » précise et prédéfinie fait l'objet de nombreuses craintes en matière de protection des données informatiques. Par exemple, la dichotomie classique « veut » que les garanties de protection juridique des données ne soient pas les mêmes selon, qu'elles sont collectées sur le territoire européen ou sur le territoire américain. Cette crainte de dispersion et de perte de maîtrise des données s'explique par le développement des outils informatiques et leur démocratisation.

3. L'informatique à l'ère de « l'homo *numericus*[6] ».- Les appareils informatiques sont devenus des objets courants de notre environnement et de notre quotidien. Néanmoins, cet univers peut paraître très technique et complexe. Selon la définition du dictionnaire de l'Académie française, l'informatique est la science « du traitement rationnel, notamment

---

[3] Les premiers « nuages » étaient construits autour du réseau lui-même sous la forme d'abstraction technique « TCP/IP », puis, les documents ont été, à leur tour, construits en nuage sous le réseau World Wide Web (www.).

[4] « La bande passante est une mesure qui définit la quantité d'information que peut véhiculer une liaison de transmission. Elle détermine la quantité d'information (en bits/s) qui peut être transmise simultanément », Glossaire, société télécom.

[5] JP. Figer, « *L'informatique en nuage* [*Cloud Computing*], *Mode ou révolution* ? », Figer.com, 25 février 2012.

[6] Termes employés dans le Rapport dit « Escoffier », « La vie privée à l'heure des mémoires numériques », M. Y. Detraine, Mme A.M Escoffier, rapport à la Commission des lois du Sénat, 27 mai 2009.

par machines automatiques, de l'information considérée comme le support des connaissances et des communications, dans les domaines technique, économique et social ». Cette définition peut être raccourcie pour n'en retenir que l'essentiel, à savoir, le traitement de l'information dans un système formel. Le traitement de l'information, contrairement à une idée répandue, n'a pas pour origine la seconde Guerre Mondiale et les célèbres Colossus ou ENIAC[7], spécialisés dans le décryptage de codes ennemis ou le calcul balistique. Sans remonter au boulier datant de 500 avant Jésus Christ, les premières machines de traitement automatisé d'informations étaient totalement mécaniques (comme les tabulatrices de 1884 utilisées pour le recensement Américain). La principale évolution se situe véritablement dans les années 1940 grâce à l'explosion des capacités de calcul, aboutissant à la création des calculateurs. C'est en 1947 que la technologie des calculateurs va devenir plus fiable. Cependant, il faut attendre le milieu des années 1960 pour voir l'informatique se développer avec les premiers circuits intégrés[8], d'abord dans les entreprises et les administrations puis, avec l'apparition des microprocesseurs, dans un usage personnel[9] pour enfin *exploser* dans les années 1970.

4. L'usage des outils informatiques a été bouleversé par le développement de l'internet, terme dérivé de « internetting ». A l'origine, l'objet de l'internetting était de relier plusieurs réseaux entre eux. L'internet est le plus grand réseau au monde. Ce dernier permet la transmission d'informations dans le monde entier via des messageries instantanées ou des courriels, mais, surtout, par l'échange d'informations via le World Wide Web (www) en permettant la consultation de documents à travers les pages web. A l'origine, l'internet apparaît dans le projet ARPANET financé par la DARPA (Agence du Ministère de la Défense Américaine) en 1965. L'objectif de ce réseau était de permettre le maintien des communications entre les réseaux militaires, de façon décentralisée, en cas d'attaque nucléaire. C'est grâce au monde de la recherche que l'Internet a été étendu à

[7] ENIAC (acronyme de l'expression anglaise Electronic Numerical Integrator Analyser and Computer), il est le premier ordinateur entièrement électronique. Il peut être reprogrammé pour résoudre, en principe, tous les problèmes calculatoires.

[8] C'est en 1958 que l'américain Jack Kilby invente le premier circuit intégré[1] créant ainsi les bases du matériel informatique moderne.

[9] Les ordinateurs personnels grand public sont apparus à la fin des années 1970 lorsque le coût et la dimension des ordinateurs ont pu être suffisamment réduits. Les premiers ordinateurs personnels populaires et souvent cités ensemble comme ayant lancé la « révolution numérique » sont l'Apple II de l'entreprise Apple, le TRS-8 de l'entreprise Tandy et le Commodore PET de l'entreprise Commodore International.

l'usage civil[10] et que le terme *Internet* est apparu et officialisé en 1983[11]. Aujourd'hui, l'utilisation de l'informatique prend différentes formes et touche la quasi-totalité des domaines d'activités : les télécommunications, la téléphonie, les données personnelles etc. Nous sommes à l'ère de « la convergence »[12] qui rassemble les technologies de l'informatique en un seul système totalement connecté. En effet, on constate aujourd'hui que les appareils regroupent des fonctions multiples et on retrouve souvent dans un seul et même appareil – un smartphone[13], par exemple - l'utilisation de médias, musique, informations, courriels, téléphonie etc. Autant d'outils qui permettent de centraliser des informations, de les collecter ou de les échanger. Ce bref historique nous permet de relever un dénominateur commun à toutes ces technologies : l'« Information ».

5. L'extension de la notion de vie privée.- La numérisation de l'information est une problématique qui est apparue à la fin des années 1970 et qui ne semblait pas créer de nouveaux risques d'atteinte à la vie privée. En effet, lorsque l'utilisation de l'informatique a débuté, la loi du 17 juillet 1970[14] renforçant la garantie des droits individuels venait de codifier une jurisprudence[15] constante en matière de protection de la vie privée. La notion de donnée à caractère personnel était considérée comme protection complémentaire du respect du droit à la privée. Cependant, c'est la révélation[16] d'un projet du gouvernement français visant à identifier chaque citoyen par un numéro et à interconnecter tous les fichiers de l'administration qui a créé une vive émotion au sein de l'opinion publique. Ce projet était connu sous le nom de Système Automatisé pour les Fichiers Administratifs (SAFARI) et a montré les risques de mésusage de l'informatique, laissant percevoir un risque de fichage général de la population. Ce constat a poussé le gouvernement à instituer

---

[10] C'est en 1969 qu'est créé le premier Network Working Group et la connexion des premiers ordinateurs entre 4 universités américaines via l'Interface Message Processor de Leonard Kleinrock.

[11] C'est l'américain Robert E. Kahn qui emploie le premier le terme « internet » lors de son intervention à Conférence Nationale des Systèmes de Communications Automatisés (ICCC) de 1972. Le terme sera officialisé pour désigner l'ensemble d'ARPANET.

[12] B. Spitz, « La révolution du numérique : l'ère de la convergence », Communication et langages, 1999, n°1, pp. 115-121, Doss. Thém. L'université d'été de la communication.

[13] Terme désignant un téléphone portable aux fonctions multimédias et pouvant se connecter à l'Internet.

[14] Loi n°70-6 du 17 juillet 1970, tendant à renforcer la garantie des droits individuels des citoyens, JORF 1970 p. 6751.

[15] De façon non exhaustive : TGI Seine, 24 nov. 1965, D. 1967. 457 ; Paris, 17 mars 1966, D. 1966. 749 ; Voir aussi sur le sujet A. Lepage, Personnalité (Droits de la), actualisation juin 2016, septembre 2009, Répertoire de droit civil, section 1.

[16] Le Monde*, « SAFARI, ou la chasse au français »,* 21 Mars 1974.

une commission, en collaboration avec le Garde des Sceaux, afin que soient mises en place des mesures garantissant que l'informatique soit développée dans les règles du respect de certains principes fondamentaux comme le respect du droit à la vie privée et des libertés individuelles. Pour cela, la Commission Nationale de l'Informatique et des Libertés (CNIL) a été créée. Depuis sa création en 1978, sa mission est d'évaluer la sensibilité des données et d'en créer une hiérarchie. La première Commission de l'Informatique et des Libertés a été présidée par Bernard Chenot. Il était chargé de créer une Autorité Administrative Indépendante (AAI). En l'absence de protection spécifique au traitement *automatisé* des données informatiques, le projet de loi avait pour objectif de créer un régime de protection des données à caractère personnel. La première mission de la CNIL était de définir les termes d'une protection des informations faisant l'objet d'un traitement automatisé. Il a été ainsi retenu la notion de protection des « données à caractère personnel » dont la définition a évolué depuis son origine. C'est à la fin de l'année 1977 qu'un projet de loi a été soumis au Parlement pour être promulgué le 6 janvier 1978[17].

I- Les sources de la protection des données à caractère personnel

§1- Les sources législatives et supra législatives de la protection

a) La Loi « Informatique et Libertés » (LIL) du 6 janvier 1978

6. L'évolution de la notion de « données à caractère personnel ».- Lors de la première rédaction de la loi de 1978, le terme de « données à caractère personnel » n'était pas formulé ainsi. En effet, la loi du 6 janvier 1978 visait les données *nominatives*. Cette formulation ne permettait donc de protéger que les données laissant apparaître le nom de la personne. Or, l'article 4 de loi originelle était rédigé en ces termes : « sont réputées *nominatives* au sens de la présente loi, les informations qui permettent, sous quelques formes que ce soit, directement ou non, l'identification des personnes [18]». Si la première rédaction peut tendre à une interprétation restrictive en raison du caractère *nominatif* des informations, l'article 4 ne vise pas uniquement la protection des informations se rapportant à l'identité de personne. La loi vise également la protection des données qui

[17] Loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978 p. 227.
[18] Article 4 de loi « Informatique et Libertés » de 1978, première rédaction.

permettent l'identification par recoupement, c'est-à-dire les informations, qui, lorsqu'elles sont isolées ne permettent pas l'identification de la personne, mais qui, lorsqu'elles sont compilées, permettent la reconstitution d'une identité. C'est à partir de ce constat que la protection des informations a été élargie lors de la présentation du rapport Braibant qui indique que « la notion de « donnée à caractère personnel » […] recouvre toute information susceptible d'être rapportée à une personne identifiée ou identifiable, [et] est beaucoup plus large que celle de donnée relative à la vie privée » ou à l'identité[19]. Le choix de cette définition paraît ainsi plus apte à protéger toutes les facettes de notre personnalité qui font l'objet d'un traitement par les Nouvelles Technologies de l'Information et de la Communication (NTIC). L'objectif de la nouvelle définition est de permettre, non seulement la protection des donnés relatives à notre identité telles que le nom, l'adresse, le numéro de téléphone ou les documents administratifs, mais, aussi, les données relatives à notre image, notre voix, notre santé ou nos données génétiques. C'est ce que souligne le rapport Braibant qui met en balance la valeur et la sensibilité des informations[20]. On remarque que, déjà, le législateur était soucieux de permettre un usage éthique des NTIC qui ont progressivement saisi les éléments qui se rapportent à notre personnalité[21], au point de créer une nouvelle « personnalité virtuelle [22]». C'est donc avec l'objectif de permettre une protection étendue que la notion d'information nominative a été remplacée par la notion de « donnée à caractère personnel ».

---

[19] Rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46 le 3 mars 1998, G. Braibant. Le rapport ajoute, d'autre part, « que le détournement des traitements de leur finalité, indépendamment de la nature des informations traitées, est susceptible d'emporter des atteintes à d'autres droits fondamentaux, comme les droits sociaux, où à la protection spécifique dont bénéficient certaines informations (secret médical, secret bancaire) ».

[20] « L'utilisation d'informations relatives aux origines raciales, aux mœurs, aux opinions politiques, philosophiques et religieuses, ou aux appartenances syndicales, emporte des risques beaucoup plus considérables que le traitement d'informations relatives à l'état-civil ou à la situation patrimoniale des personnes, notamment dans la mesure où elle met en jeu d'autres droits fondamentaux : la liberté d'opinion, la liberté de conscience, ou l'interdiction de toute discrimination en raison de ces caractères. Ces données sensibles, dont le champ est plus étroit que celui de la vie privée, doivent donc jouir d'une protection exceptionnelle. Leur traitement doit être regardé comme illégitime par nature, sauf dans des cas très particuliers, comme la tenue par les églises et les groupements à caractère religieux, philosophique et syndical de registres de leurs membres, ou pour des motifs d'intérêt public et sous réserve de garanties renforcées ». Rapport Braibant op. cit. loci.

[21] N. Weinbaum, *« Les données personnelles confrontées aux objets connectés »*, Comm. Com. Electr. N°12, décembre 2014, étude n°22 ; F. Stéfani, « *le secret médical à l'épreuve des nouvelles technologies »,* Recueil Dalloz 2009, page 2636.

[22] Rapport du Conseil d'Etat, « *Internet et les réseaux numériques »* du 2 juillet 1998 ; Rapport du Conseil d'Etat « *Le numérique et les droits fondamentaux »,* étude annuelle 2014, La Doc. Fr. Coll. Rapports publics, page 1440.

7. Ainsi, le rapprochement de la notion de vie privée paraît inévitable en raison du nombre de composantes de notre vie personnelle qui sont captées par les outils informatiques. En effet, les NTIC doivent permettre un usage dans le respect du droit à la vie privée *classique*, c'est-à-dire les informations relatives au nom, à l'adresse etc. ; mais aussi un usage dans le respect du droit à la vie privée *moderne* avec les données relatives à la voix, à l'image et, plus largement, la notion de protection doit tendre à la protection des données relatives à notre mode vie comme l'appartenance religieuse, nos déplacements, nos opinions politiques, notre orientation sexuelle et notre état de santé.

8. Le contenu de la loi «Informatique et Libertés».- Le second apport de la « LIL » de 1978 est la définition des contours de la notion de « traitement automatisé » qu'elle a permis. La première rédaction de la « LIL » définissait un traitement automatisé comme « tout ensemble d'opérations réalisé par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives, ainsi que tout ensemble d'opération de même nature se rapportant à l'exploitation de fichiers ou base de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives [23]». Il convient de compléter la définition en indiquant que le champ d'application de la loi ne se limite pas seulement aux traitements automatisés. En effet, le texte vise également la protection des données qui font l'objet d'un traitement manuel[24] ou mécanique. La loi permet de protéger un grand nombre de cas de traitement de données. Cette définition large de la notion de donnée à caractère personnel est également partagée par la CNIL qui retient la qualification de donnée à caractère personnel dès qu'un risque d'atteinte à la vie privée est constitué[25]. Il semble donc que la notion de donnée à caractère personnel doive être interprétée de la façon la plus large possible afin de prévenir tout risque d'atteinte à la vie privée. C'est la définition issue de la directive européenne du 26 octobre 1995[26], sur laquelle nous reviendrons tout au long du développement, qui semble le mieux recouvrir la diversité des données à caractère personnel et qui sera transposée en droit français par la

[23] Article 5 de la loi « Informatiques et Libertés » originelle op. cit. loci.
[24] Article 45 ibidem note précédente.
[25] Cf infra, Section 2, les données sensibles permettant la déduction d'informations sensibles. Page 82.
[26] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050.

loi du 6 août 2004[27]. Ainsi, la directive définit les traitements de données à caractère personnel comme « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction[28] ».

Les deux notions exposées ci-dessus sont des notions fondamentales car elles constituent le socle de la protection qui impose, par principe, que tout traitement informatique de données doit être soumis au régime de protection de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

9. La distinction des traitements selon le secteur.- La loi «Informatique et Libertés» prévoyait, à l'origine, un régime de protection différent selon que le traitement était effectué par le secteur public ou privé. Les traitements de données à caractère personnel dans le secteur public étaient plus contraignants. Ceux-ci étaient visés à l'article 15 de la « LIL » qui prévoyait que, en dehors d'une autorisation légale, le texte réglementaire devait être soumis à l'avis de la CNIL qui ne pouvait être contourné que par décret pris avec avis du Conseil d'Etat. Dans le secteur privé, le régime prévoyait que les traitements de données étaient uniquement soumis à déclaration auprès de la CNIL et la licéité du traitement était subordonnée à la réception du récépissé[29]. De plus, pour les traitements les plus courants, un système de déclaration simplifiée était prévu.

La réforme de la « LIL » par la loi du 6 août 2004 a atténué cette distinction de régime alors que le nombre de textes législatifs créant de nouveaux fichiers a entrainé une diminution de la protection prévue par la « LIL ». En effet, si la plupart des avis de la Commission n'étaient pas défavorables, la création de fichiers n'était pas soumise à un avis conforme de la CNIL. Néanmoins, la Commission n'hésite pas à émettre des réserves et à exiger des garanties supplémentaires mais le législateur ne semble pas toujours enclin à

[27] 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 modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004 page 14063.
[28] Article 2 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050.
[29] CE, 6 janvier 1997, Caisse d'épargne Rhône-Alpes Lyon contre CNIL, n°159129.

prendre en considération ses remarques. Cette situation inquiète parfois la CNIL car son rôle n'est pas toujours mis en avant[30]. On se souvient du communiqué de la Commission datant du 16 février 2006 et concernant la loi antiterrorisme où elle dénonçait certaines mesures sur lesquelles elle avait émis des réserves n'ayant pas été prises en compte. Il semble que le rôle de la CNIL soit quelque peu ignoré alors que la sensibilité des données traitées paraît évidente. Lors de la mise en place du Dossier Médical Personnel (DMP), il était prévu d'attribuer un numéro unique à chaque titulaire d'un DMP. Ce numéro devait être créé et attribué à partir du Numéro d'Inscription au Répertoire (NIR) mais la CNIL affirme qu'elle n'a pas fait l'objet d'une consultation pour la mise en place d'un tel numéro[31]. On retrouve ici des similitudes avec les craintes suscitées par la mise en place du projet SAFARI.

Les textes de loi précités sont le fruit de la volonté de la Commission Nationale de l'Informatique et des Libertés dont les missions et les pouvoirs font l'objet d'un chapitre entier au sein de la « LIL ». Cette autorité a un pouvoir décisionnel et est indépendante. Ses décisions peuvent faire l'objet d'un recours devant le Conseil d'Etat.

10. La création d'une autorité de contrôle.- La Commission Nationale de l'Informatique et des Libertés a été créée par le décret n° 74-230 du 7 mars 1974. Le contexte dans lequel la Commission a vu le jour illustre bien sa raison d'être, en lien avec cette étude. C'est le célèbre projet SAFARI[32], qui permettait le fichage des individus au travers de l'utilisation d'informations recueillies par la police ou l'assurance maladie, qui a poussé le législateur à créer une autorité indépendante spécifique à la protection des données personnelles collectées par un système automatisé.

Le premier rapport de 1975[33] faisait état de plusieurs propositions nécessaires à l'usage et à la maîtrise de l'informatique, notamment sur la nécessité d'élaborer une loi spécifique à l'usage de l'informatique, avec la mise en place d'un « organe collégial

[30] J-L. Autin, « Le devenir des autorités administratives indépendantes, RFDA 2010 p. 875.
[31] CNIL, délibération n°2010-449 du 2 décembre 2010, portant autorisation des traitements de données personnelles mis en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel.
[32]SAFARI : acronyme de Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus Op. Cit. Loci.
[33] Rapport rendu sous le nom du rapporteur général M. Bernard Tricot, 27 juin 1975, Le Doc. Fr. Coll. Rapports publics.

indépendant chargé de veiller à l'application de la loi ». Ces recommandations ont servi de base à la création de la (CNIL) ainsi qu'à la création de la loi du 6 janvier 1978[34].

L'article 21 de la loi du 6 janvier 1978 dispose que la CNIL est une Autorité Administrative Indépendante (AAI) qui ne reçoit d'instructions d'aucune autre autorité[35] et dispose des crédits nécessaires à l'accomplissement de ses missions[36].

La mission générale de la CNIL est un devoir d'information à l'égard du public concerné par le traitement des informations à caractère personnel. Les dispositions de la loi du 6 janvier 1978 indiquent que la CNIL remplit une mission de contrôle, d'élaboration et de mise en œuvre de traitement des informations, *a priori,* mais également, *a posteriori,* comme en dispose l'article 11 de la loi n°78.17 du 6 janvier 1978 qui donne à la Commission le pouvoir de veiller « à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi. ». Les traitements automatisés portant sur les données génétiques sont soumis à une autorisation préalable de la Commission, mais, également, lorsque l'objet du traitement doit permettre « l'interconnexion de fichiers »[37]. Dans le cadre de cette étude, la CNIL interviendra notamment pour le déploiement des Référentiels Généraux de Sécurité (RGS) et des Référentiels Généraux d'Interopérabilité (RGI) comme en dispose l'ordonnance du 8 décembre 2005[38].

Toujours dans le cadre de sa mission d'information et de contrôle, la CNIL est compétente pour recevoir « les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci »[39]. La loi «Informatique et Libertés» donne pour principale mission à la CNIL de s'assurer que les traitements de données personnelles respectent les conditions suivantes :

> «1- Les données sont collectées et traitées de manière loyale et licite ;
>
> 2- Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche

[34] Loi n°78.17 su 6 janvier 1978 op.cit.
[35] Article 21 de la loi n°78.17 su 6 janvier 1978.
[36] Article 12 de la même loi, ses crédits sont soumis au contrôle de la Cour des comptes.
[37] Article 25 de le loi 78.17 du 6 janvier 1978.
[38] L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
[39] Op. Cit. Article 11 de la loi 78.17 du janvier 1978.

scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus […] et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3- Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

4- Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

5- Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées[40]. »

Ces conditions nous serviront de guide tout au long de cette étude. Il convient également de souligner que, parmi les conditions de traitement, le consentement de la personne prime, comme en dispose l'article 7 de la loi «Informatique et Libertés» :

« Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

1- Le respect d'une obligation légale incombant au responsable du traitement ;

2- La sauvegarde de la vie de la personne concernée ;

3- L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

4- L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

[40] Article 6 de la loi 78.17 du 6 janvier 1978.

5- La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. »

Dans le cadre de la loi, le consentement est une information supplémentaire qui doit être recueillie pour que les informations sur l'état de santé soient collectées, échangées ou partagées. Par exemple, on peut rapprocher cette condition du Code de la santé publique dans lequel le respect du consentement du patient fait l'objet d'une attention particulière par le législateur concernant la notion de respect de la personne et du secret médical[41].

Par ailleurs, la CNIL est dotée d'un pouvoir de sanction prévu aux articles 45 et suivants de la loi n°78-17 du 6 janvier 1978. Elle peut prononcer un avertissement à l'égard du responsable d'un traitement qui ne respecterait pas les conditions et obligations découlant de la loi. Elle peut également saisir la juridiction compétente pour ordonner des mesures de mise en conformité à la loi, en cas d'atteinte grave aux libertés visées à l'article 1 de la loi. Elle peut émettre des sanctions pécuniaires proportionnelles à la gravité des manquements. Enfin, l'article 51 de la loi «Informatique et Libertés» prévoit que des sanctions pénales puissent être prononcées en cas d'entrave à l'action de la Commission ou à l'exercice des fonctions de ses membres.

La CNIL apparaît donc comme l'autorité de référence en matière de traitement des données à caractère personnel car elle est amenée à traiter tous les domaines saisis par l'informatisation des données à caractère personnel. La « LIL » a donc créé non seulement une autorité de contrôle originale, mais, elle consacre également trois principes essentiels.

11. Le droit à l'information.- Le principe du droit à l'information est visé à l'article 3 de la « LIL ». C'est une notion centrale sur laquelle nous reviendrons dans le développement. Ce principe permet à toute personne dont les données font l'objet d'un traitement informatique, d'avoir connaissance des informations détenues par un prestataire de services électroniques ou, plus généralement, de savoir quelles informations sont utilisées et conservées par le responsable du traitement. Le droit à l'information a fait l'objet d'une évolution et d'un renforcement depuis la promulgation de la « LIL » en 1978.

[41] Code de la santé publique articles : L. 1110-4, L1111-4, L. 1111-8.

En effet, la nouvelle réforme[42] du cadre européen consacre une obligation renforcée qui pèse sur le responsable du traitement. Ainsi, le responsable devra prouver qu'il a employé tous les moyens pour assurer l'information de la personne concernée par le traitement. Le droit à l'information pourrait être qualifié de « clé de voute » de la protection des données à caractère personnel car il conditionne l'exercice de deux autres principes que sont le droit d'opposition et le droit d'accès.

12. Le droit d'opposition.- Visé à l'article 26 de la loi[43], le droit d'opposition permet à une personne de s'opposer, pour des raisons légitimes, à ce que ses données personnelles fassent l'objet d'un traitement informatique. Ce droit peut s'apparenter à un retrait du consentement de la personne concernée. Il fait, lui aussi, l'objet d'un renforcement par la réforme du cadre de protection des données au niveau européen, bien qu'il ait été repris par la directive européenne de 1995. Cependant, ce droit connaît des restrictions, notamment en ce qui concerne les fichiers détenus par l'administration fiscale, par les services de police et de gendarmerie et par la justice. Le droit d'opposition apparaît comme la prérogative essentielle de la protection du consentement.

13. Le droit d'accès et de rectification.- Visé aux articles 34 à 40 de la « LIL », ce droit permet à la personne concernée par le traitement de vérifier l'exactitude de ses informations. Dans le cas où celles-ci seraient inexactes ou périmées, la personne peut adresser au responsable du traitement une demande visant à les mettre à jour. Elle peut également demander à ce qu'elles soient effacées.

Néanmoins, la protection des données à caractère personnel ne saurait être limitée au respect de ces trois principes. D'autres droits, tels que le droit à l'oubli et la force du consentement, doivent faire l'objet d'une attention particulière et bénéficient d'une protection croissante dans les autres sources garantissant la protection des données personnelles.

---

[42] Règlement (UE) 2016/679 du Parlement européen et du Conseil européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), JOUE L. 119/1

[43] Article 26 de loi « Informatique et Libertés » de 1978 op. cit .loci.

b) La directive 95/46/CE de 1995 : l'harmonisation et la reconnaissance de la protection des données à caractère personnel

Il serait difficile de reprendre de façon exhaustive les mécanismes de la directive européenne du 24 octobre 1995 tant celle-ci a impliqué de nombreux changements sur le plan international. A ce stade du développement, nous nous attacherons à présenter et définir les principaux objectifs du texte européen.

14. L'harmonisation des moyens de protection au sein de l'Union Européenne.- Le considérant n°7 de la directive permet de connaître le contexte dans lequel la directive a été élaborée :

> « Considérant que les différences entre États membres quant au niveau de protection des droits et libertés des personnes, notamment du droit à la vie privée, à l'égard des traitements de données à caractère personnel peuvent empêcher la transmission de ces données du territoire d'un État membre à celui d'un autre État membre; que ces différences peuvent dès lors constituer un obstacle à l'exercice d'une série d'activités économiques à l'échelle communautaire, fausser la concurrence et empêcher les administrations de s'acquitter des responsabilités qui leur incombent en vertu du droit communautaire; que ces différences de niveau de protection résultent de la disparité des dispositions nationales législatives, réglementaires et administratives. »

Les motifs qui ont incité à la rédaction de la directive répondent à une crainte suscitée par la multiplication du nombre de lois visant la protection des données à caractère personnel[44] en Europe. Ainsi, en se référant aux textes et normes adoptés par l'Organisation des Nations Unies[45] (ONU) et l'Organisation de Coopération et de

[44] La loi fédérale du 20 décembre 1990 sur la protection des données, modifiée ultérieurement, a remplacé la loi du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement des données. Avec la loi fédérale de 1977, l'Allemagne avait été le premier pays à se doter d'un texte général sur la protection des données personnelles ; Loi belge du 8 décembre 1992 (Loi vie privée) vise à protéger le citoyen contre toute utilisation abusive de ses données à caractère personnel. Elle définit non seulement les droits et devoirs de la personne dont les données sont traitées, mais, aussi, ceux du responsable d'un tel traitement ; en Suède loi relative aux « datalag » du 11 mai 1973.

[45] Résolution n°45/95 adoptée par l'Assemblée Générale des Nations Unies, le 14 décembre 1990, relative à la collecte et la gestion d'informations à caractère personnel. Elle définit les principes essentiels en matière de traitement de données à caractère personnel. Ces principes sont au nombre de dix.

Développement Economique[46] (OCDE), le Parlement et le Conseil de l'Europe ont enclenché le processus de rédaction de la directive 95/46/CE sur la protection et la circulation des données à caractère personnel au sein de l'Union Européenne. Outre les textes précités, le Conseil et le Parlement s'appuient sur la Convention n°108 adoptée par le Conseil de l'Europe le 28 janvier 1981, pour élaborer la directive européenne. La convention n°108, consacre, notamment, un mécanisme important qui interdit la communication des données aux Etats qui ne disposent pas d'une protection suffisante en matière de traitement des données à caractère personnel. Si ce texte est cité comme référence, c'est en raison de sa portée. En effet, la ratification de la Convention n'est pas limitée aux seuls membres du Conseil de l'Europe. Il s'agit donc du « premier instrument international contraignant qui a pour objet de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel et qui réglemente les flux transfrontaliers des données[47] ».

C'est donc avec l'objectif de concilier des philosophies juridiques parfois opposées et sur le fondement de l'article 100 (ancien) du traité instituant la Communauté Européenne, que la directive européenne a été élaborée, dans le but de réaliser et d'harmoniser le marché intérieur. On remarque également que c'est avec l'objectif de respecter deux principes difficiles à concilier que la directive a été rédigée : d'un coté, la souveraineté des Etats membres limite la portée du droit européen, et, de l'autre, la directive vise à garantir la protection des données personnelles tout en assurant leur libre circulation.

15. Le respect de la souveraineté des Etats.- C'est en la présentant sous l'angle de la nécessité de mettre en œuvre le « même niveau de sécurité » garanti dans tous les pays que la directive de 1995 vise à l'harmonisation des moyens de protection des données à caractère personnel. En effet, le considérant n°8 indique que la transposition du texte européen vise à garantir une sécurisation de « principe[48] » et « complète[49] ». Les articles 10, 11 et 25 de la directive prévoient qu'il est laissé à la discrétion des Etats de définir les données qui pourront faire l'objet d'un transfert entre Etats qui prévoient le même niveau

[46] Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980. Les lignes directrices sont édictées sous forme de recommandations.
[47] Résumé de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ouvert à la signature des Etats membres et à l'adhésion des Etats non membres. Référence STE n°108 du 28 janvier 1981, disponible sur http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108.
[48] Considérant n°8 de la directive de 1995 op. cit. loci.
[49] Ibidem.

de garantie de protection. C'est donc dans l'optique d'éviter le transfert dans des « paradis numériques[50] » que la directive européenne prévoit la mise en place d'un niveau de « protection adéquate[51] ».

C'est avec la même ambition de créer une cohésion entre les Etats membres que l'article 29 de la directive a créé le « Groupe de travail de l'article 29 » dit « G29 ». Le groupe de travail réunit l'ensemble des autorités publiques et est chargé de veiller à la bonne application de la réglementation relative à la protection des données à caractère personnel. C'est tout naturellement que la CNIL siège durant les travaux du groupe de travail. Le G29 a pour mission de réaliser un rapport annuel concernant la cohérence de la mise œuvre de la coordination et de la réglementation. Le groupe de travail a également pour mission de reconnaître et d'évaluer les réglementations et les mesures de sécurité mises en place par les Etats. Les avis du G29 nous serviront de base de réflexion tout au long de notre étude.

16. Garantir la libre circulation des données.- Outre la mise en place du niveau adéquat de protection pour le transfert de données entre les Etats membres et les pays tiers, la directive est complétée par plusieurs autres directives qui concernent différents secteurs d'activité. Par exemple, elle est assortie de la directive du 15 décembre 1997[52], relative aux télécommunications, modifiée par la directive du 12 juillet 2002[53]. Sans viser de façon exclusive la protection des données à caractère personnel, de nombreux textes prévoient des dispositions qui concernent le domaine de la protection des données à caractère personnel[54].

Les objectifs de la directive européenne de 1995 ne se limitaient cependant pas à garantir la protection des données personnelles dans le respect de la souveraineté de

---

[50] J. Frayssinet « *Le transfert et la protection des données personnelles en provenance de l'Union européenne vers les Etats-Unis : l'accord dit « sphère de sécurité ou Safe Harbor »,* JCP, Comm. Com. Electr., mars 2001, page 10.

[51] Article 25 de la directive européenne op.cit. loci.

[52] Directive 97/66/CE du Parlement et du Conseil, du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

[53] Directive 2002/58/CE du Parlement et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques dite directive vie privée et communications électroniques.

[54] Par exemple : Directive n°97/7du 20 mai 1997 sur la protection des consommateurs en matière de contrat à distance ; la directive n°2000/31 du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information et, notamment, du commerce électronique dans le marché intérieur.

chaque Etat. Elle a consacré de nouveaux principes qui ont été repris lors de la transposition de la loi française du 6 août 2004.

17. L'obligation du responsable du traitement de garantir la *qualité* des données.- L'article 6 de la directive vise les conditions de licéité du traitement en définissant les obligations du responsable de traitement. En effet, le responsable a l'obligation de collecter et de traiter les données de façon loyale, pertinente et conforme à la finalité du traitement. Ces obligations se rapportent aux législations préexistantes des Etats membres. L'article 7 précise les fondements pouvant légitimer le traitement des données. Ainsi, le traitement est légitime, soit lorsque la personne a « indubitablement » donné son consentement, soit lorsque ce traitement est nécessaire à l'exécution d'un contrat dont la personne concernée est partie, soit lorsqu'il répond à une obligation légale[55] à laquelle le responsable du traitement doit se conformer. Cette disposition est originale vis-à-vis du droit français car la place du consentement y est forte. C'est l'interprétation de la dernière disposition qui a, toutefois, suscité le plus d'interrogations lors de la transposition par la loi du 6 août 2004. En effet, il a été difficile de mettre en balance la réalisation de l'intérêt légitime du traitement et le respect des droits et libertés fondamentales. De plus, les articles 16 et 17 de la directive prévoient un droit à la sécurité et à la confidentialité des données. En d'autres termes, le responsable du traitement doit prévoir des mesures de sécurité afin d'éviter « la destruction, l'altération, l'accès ou la diffusion des données ». Il revient au responsable du traitement de s'assurer que les sous-traitants auxquels il fait appel respectent les conditions de sécurité auxquelles il est lui-même tenu. Cette obligation du responsable du traitement fait notamment appel au respect du secret professionnel auquel il doit se conformer. Il doit veiller à ce que ses collaborateurs s'y conforment également.

18. Le renforcement des droits des personnes.- L'article 12 de la directive de 1995 prévoit que la personne concernée par le traitement peut « sans contrainte », « sans délai » et « sans frais » obtenir l'information sur les données qui font l'objet d'un traitement, la finalité de celui-ci et avoir connaissance des destinataires. Elle peut également exiger d'avoir connaissance de l'origine des données ainsi que la « logique que sous-tend le traitement ». La directive de 1995 consacre donc le droit de la personne d'obtenir la rectification, l'effacement ou le verrouillage de ses données. Ce droit est assorti de

[55] Le traitement est justifié par la sauvegarde de l'intérêt vital de la personne concernée ou répond à une mission d'intérêt public ou de l'exercice de l'autorité publique.

l'obligation, pour le responsable du traitement, de notifier aux tiers l'exercice de ces prérogatives. Il lui incombe également la charge de prouver que cette notification a bien été transmise.

De même, lorsque le traitement des données n'est pas fondé sur l'expression du consentement, l'Etat doit garantir à la personne un droit d'opposition qui doit être fondé sur des motifs légitimes de s'opposer à ce traitement. Cette disposition ressemble au droit d'opposition [56] de la « LIL » de 1978. Cependant, la directive laisse le choix aux Etats qui peuvent prévoir une situation contraire, c'est-à-dire que le droit d'opposition peut être exercé sans motif légitime[57].

Enfin, l'article 8 de la directive prévoit l'application de règles spécifiques lorsque le traitement concerne certaines catégories de données sensibles. Ainsi, les données relatives aux origines raciales ou ethniques, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données relatives à la santé ou à la vie sexuelle font l'objet d'une protection consacrée au niveau européen. Les données énumérées précédemment font donc l'objet d'un traitement seulement dans les cas énumérés par l'article 8 de la directive.

19. En France, le projet de loi visant la transposition de la directive 95/46/CE a fait l'objet de nombreuses modifications, notamment concernant l'ajout de certaines interdictions. En effet, l'ajout des exceptions énumérées par l'article 8 de la directive a posé quelques difficultés[58]. Néanmoins, certains apports tels que la désignation du Correspondant Informatique et Libertés (CIL) par certaines personnes morales ont créé de véritables mécanismes protecteurs. Il serait vain, à ce stade, d'énumérer toutes les dispositions qui ont fait l'objet d'une transposition sans risquer de recopier littéralement la loi du 6 août 2004. Les différentes dispositions de la directive reprises au sein de la loi du 6 août 2004 seront exposées et analysées tout au long du développement. Enfin, il convient de présenter la nouvelle réforme européenne qui a adopté, le 27 avril 2016, le Règlement[59]

---

[56] Article 56 de la « LIL » modifiée.
[57] Article 14 de la directive européenne op. cit. loci.
[58] Voir les travaux préparatoires déposés à l'Assemblée Nationale le 9 janvier 2002 et le rapport Gouzes sur le projet de loi N° 3250, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, du 9 janvier 2002.
[59] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

renforçant les droits de la personne concernée par le traitement de ses données personnelles.

c) Le Règlement 2016/679/UE du 27 avril 2016

20. Le renforcement *nécessaire* de la protection des données.- Les considérants n°6 et n°7 du nouveau texte européen justifient la nécessité de renforcer la protection des données à caractère personnel en indiquant que « l'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel ». Ces nouveaux enjeux « requièrent un cadre de protection des données solide et plus cohérent dans l'Union ». Le considérant n°7 du Règlement reflète le caractère obsolète de la directive de 1995. Cette obsolescence est, très certainement, due à l'évolution des technologies de l'information qui a considérablement changé les modes de collecte de données. Elle est également justifiée par le fait que les TIC sont omniprésents dans la vie de chaque citoyen européen. En outre, le même considérant insiste sur la nécessité de réaliser un cadre de protection des données harmonisé, notamment par l' « application rigoureuse des règles ».

21. La révision controversée de la directive 95/46/CE.- En 2008, lors de la proposition de révision de la directive de 1995, la Commission européenne a souhaité mettre en place un comité d'experts afin de déclencher le processus de réflexion du projet de réforme de la protection des données à caractère personnel. La composition du comité a fait l'objet d'une vive polémique. En effet, seul un membre[60] du comité était issu d'une autorité de contrôle européenne ; il s'agissait du vice président du groupe de travail de « l'article 29 ». Les quatre autres membres[61] désignés pour siéger étaient issus des firmes américaines *Google* et *Intel* ou de cabinets d'avocats et « lobbyistes dont les maisons mères sont situées aux Etats-Unis » comme le déplorait l'ancien président de la CNIL, A.

[60] J. Kohnstamm, président de la Dutch DPA (équivalent de notre CNIL) aux Pays-Bas et vice-président du groupe dit « de l'article 29 » des institutions nationales européennes en charge de la protection des données.

[61] Le comité d'experts se composait de : D. Hoffman, responsable sécurité et vie privée chez Intel, et ancien conseiller de la Fédéral Trade Commission ; P. Fleischer, ancien responsable de Microsoft et responsable des questions liées aux données privées chez Google ; H. Tielemans avocate et lobbyiste belge du cabinet juridique américain Covington & Burling LLP (Washington DC) ; Ch. Kuner, avocat bruxellois du cabinet américain Hunton & Williams (Virginie), un des cinquante plus gros cabinets d'affaires au monde.

Türk[62]. Lors des débats, ce dernier insistait sur le « conflit transatlantique » qui existe en matière de concept de « donnée à caractère personnel ». En effet, l'ancien président de la CNIL affirme que les géants d'internet comme *Facebook* considèrent qu'ils ont un droit de propriété « à vie » sur les données des utilisateurs. A. Türk continue son raisonnement en indiquant que les CNIL européennes ont reproché aux géants américains « de croiser les adresses IP avec les informations comportementales » pendant 2 ans.

La position des CNIL européennes est devenue d'autant plus ferme lorsque A. Türk a évoqué l'informatisation de certaines données sensibles telles que les données de santé et la mise en place des dossiers médicaux numériques[63]. C'est donc avec le soutien du Conseil National de l'Ordre des Médecins (CNOM) que la nécessité de revoir la composition du comité d'experts a été demandée car « l'informatisation de la santé en France, notamment par la mise en place d'un Dossier médical informatisé du patient, impose une protection rigoureuse des données personnelles de santé, le CNOM et le CISS ne peuvent que s'alarmer des conditions d'expertise par lesquelles la Directive européenne de 1995 serait révisée ».

Cette polémique concernant la composition du comité d'experts pour la révision de la directive 95/46/CE a été soulevée[64] en France en 2009, au Sénat. Face à l'opposition, le secrétaire d'Etat chargé des affaires européennes a répondu que les autorités françaises avaient décidé de lancer « plutôt une large consultation afin de renforcer la protection des données et de réfléchir à l'éventuelle nécessité de moderniser le cadre juridique existant. [65]». Cédant à la pression, la Commission a alors décidé de dissoudre le Comité

---

[62] Alex Türk alerte contre les conditions de révision de la Directive de 1995 relative à la protection des données personnelles, I-MED, Rev. NTIC 2009, n°311.

[63] L'argument de l'ancien président de la CNIL est on ne peut plus clair : « A l'heure où la firme de Mountain View (Californie) avec Google Health et le géant de Redmond (Washington DC) avec HealthVault, se lancent dans les dossiers médicaux en ligne, il y a de quoi être inquiet pour nos précieuses données de santé, un nouveau gisement à exploiter, car leur protection juridique est du même tonneau que les informations hébergées par les autres géants américains de l'internet , c'est à dire proche de zéro ! »

[64] Question écrite n° 07430 de M. I. Renar, publiée au JO Sénat du 12/02/2009 - page 351.

[65] Réponse du Secrétariat d'État chargé des affaires européennes publiée au JO Sénat du 12/03/2009, page 627 : « *Le 12 juin 2008, la Commission avait en effet lancé un appel à manifestation d'intérêt en vue de la création d'un « groupe d'experts pour la protection des données dans l'Union européenne », destiné à l'assister dans sa réflexion sur l'opportunité de nouvelles propositions législatives. Les informations concernant la composition de ce groupe ont légitimement suscité des interrogations dont la Commission n'a pas manqué d'avoir connaissance. C'est donc avec intérêt que les autorités françaises ont relevé les déclarations du vice-président Jacques Barrot et son intention, exprimée encore récemment dans l'intervention prononcée le 28 janvier 2009 pour la « troisième journée de la protection des données », de lancer plutôt une « large consultation » afin de renforcer la protection des données et de réfléchir à l'éventuelle nécessité de moderniser le cadre juridique existant. Il est donc désormais prévu que la réflexion*

d'experts en admettant la nécessité de mettre en place « une instance composée de manière équilibrée et pluraliste[66] ».

22. La proposition de Règlement du 25 janvier 2012.- La Commission a rendu publique une proposition de Règlement modifiant le cadre de la protection des données à caractère personnel au sein de l'Union européenne[67]. Les principaux apports avaient été définis par la Commission dans un communiqué du 4 novembre 2010[68]. La Commission y indiquait que la refonte du cadre de protection européen des données à caractère personnel devait permettre de mieux répondre à l'évolution constante et rapide des nouvelles technologies, et, ceci, dans le souci d'éviter la fragmentation[69] de la protection des données au sein de l'UE. Le besoin d'harmoniser les instruments juridiques de protection fonde le choix de la norme réglementaire. La valeur contraignante d'un Règlement plutôt qu'une directive est une réponse au désaccord exprimé par certains pays à ce que la directive soit abrogée, évitant ainsi les risques de failles de la protection des données au sein de l'UE.

23. Le champ d'application du nouveau texte.- Le Règlement européen engage une véritable révolution en ce qui concerne son champ d'application territorial. En effet, le Règlement s'appliquera que le responsable du traitement se trouve au sein de l'Union Européenne ou en dehors. L'apport remarquable est la consécration du guichet unique permettant de centraliser la compétence des autorités de contrôle. Ainsi, l'autorité de contrôle de l'Etat membre sera compétente là où se situe l'établissement principal du responsable du traitement. Le Règlement européen va dans le sens d'une protection accrue

---

sur une révision de la directive de 1995 soit conduite dans le cadre d'une consultation plus large, selon des modalités qui sont encore à définir et sur lesquelles nous devrons naturellement rester vigilants. »

[66] Commission des lois du Sénat, Communiqué du 18 février 2009, « Groupe d'experts sur la protection des données en Europe : La commission des lois du Sénat souhaite son remplacement par une instance composée de manière équilibrée et pluraliste ».

[67] Proposition de Règlement du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données) / COM/2012/011 final - 2012/0011 (COD). Du 25 janvier 2012.

[68] Communication de la Commission au Parlement Européen, au conseil, au Comité Economique et Social Européen et au Comité des Régions «Une approche globale de la protection des données à caractère personnel dans l'Union européenne». COM (2010) 609 final, le 4 novembre 2010.

[69] G29, Rapport WP 106, relatif à l'obligation de notification aux autorités nationales de contrôle sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union Européenne, adopté le 18 janvier 2005, voir aussi l'avis 10/2004 WP 100, relatif aux dispositions davantage harmonisées en matière d'information, adopté le 25 novembre 2004.

des personnes puisque le texte prévoit que cette protection s'applique, même si le responsable du traitement est établi en dehors de l'UE et qu'il propose des biens et des services à une personne domiciliée au sein de l'UE[70].

24. Les obligations *renforcées* du responsable du traitement.- Le Règlement européen met le responsable du traitement au centre du mécanisme de protection des données. En effet, il ne devra plus s'acquitter des formalités préalables prévues par la directive de 1995 que certains auteurs jugeaient imprécises[71], mais, il devra tenir et rendre compte d'une liste des traitements effectués assortie d'une analyse d'impact sur la personne. De plus, lorsque le traitement atteint un certain seuil de personnes concernées, il devra obligatoirement désigner un Délégué à la Protection des Données (DPD). En outre, l'obligation de sécurité est reprise par le Règlement, mais, elle étend l'obligation de notifier la violation des données à caractère personnel, prévue par la directive 2002/58/CE[72], à tous les responsables du traitement. Le Règlement européen marque véritablement la volonté du législateur européen de renforcer les droits des personnes, notamment en renforçant l'obligation d'information à l'égard de la personne concernée par le traitement.

25. Le renforcement des droits des personnes.- Le nouveau texte réglementaire européen marque l'avènement d'une normalisation des règles d'information. Cette normalisation est marquée par l'obligation du responsable du traitement de se conformer aux mécanismes d'information instaurés par le « *privacy by design* ». Il s'agit d'une obligation qui impose au responsable du traitement de mettre en œuvre toutes les mesures de sécurité nécessaires « dès la conception du traitement ». Ce mécanisme vient compléter la protection des données par défaut (*privacy by default)* et renforce la protection du droit à la vie privée qu'implique l'usage des nouvelles technologies (*Privacy Enhanced Technology).*

Le renforcement des contraintes vis-à-vis du responsable du traitement vise surtout à garantir les prérogatives de la personne concernant son droit à être informée. Le droit à

---

[70] Cette disposition avait été déjà proposée dans la résolution législative du Parlement européen du 12 mars 2014 sur la Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données COM(2012) 0011, amendement n°98.

[71] N. Metanillos « *Réforme du cadre européen de la protection des données à caractère personnel : où en est on ?* » RDLI 2013, n°99, 3303.

[72] Directive dite « communication est vie privée » de 2009, op. cit. loci.

l'information fait l'objet d'un renforcement et approfondit les dispositions de la directive n°95/46/CE. En effet, lorsque les informations sont transmises à la personne concernée, la durée de conservation, l'origine et les conséquences du traitement envisagé (étude d'impact[73]) doivent être mentionnés. De plus, le responsable du traitement sera contraint de répondre aux demandes d'informations en respectant la forme d'émission de celles-ci. C'est-à-dire que le responsable devra fournir les informations par voie électronique si la personne concernée a employé ce mode de communication. En ce qui concerne le droit d'accès et de rectification, le Règlement prévoit que ces droits devront être gratuits alors que la directive prévoyait la possibilité de faire peser des « frais non-excessif » sur la personne concernée. Une évolution importante est à noter en ce qui concerne le droit d'opposition. En effet, le Règlement inverse la charge de la preuve d'un motif légitime pour s'opposer au traitement. Par conséquent, il appartiendra au responsable du traitement de démontrer les motifs légitimes justifiant la conservation et le traitement des données.

26. La consécration du droit à l'oubli numérique.- Consacré par l'article 14 du Règlement européen sous la formulation de « droit à l'effacement », le texte Règlementaire consacre l'arrêt dit « *Google Spain*[74] ». Cet arrêt vise notamment à protéger la personne concernée lorsque ses données sont diffusées sur les réseaux sociaux, périmées ou constitutives d'une discrimination. Cet arrêt affirme que les données dont la finalité est remplie doivent être supprimées. Cet arrêt vaut également lorsque le consentement qui fondait le traitement a été retiré ou lorsque la durée de conservation des données est arrivée à son terme.

27. Le droit à la portabilité.- Le Règlement européen consacre également le droit pour la personne concernée de *récupérer* ses données afin qu'elle puisse les confier à un autre responsable du traitement (en réalité un autre prestataire) lorsqu'elle le désire. Outre la consécration du droit de disposer de ses données personnelles, cette disposition est une véritable consécration de la place du consentement. En effet, le texte européen prévoit que le droit à la portabilité des données trouve à s'appliquer lorsque le consentement était requis pour la mise en œuvre du traitement et qu'il en fondait la légitimité.

---

[73] G29, Avis 05/2014 sur les techniques d'anonymisation, 10 avril 2014.
[74] CJUE, Arrêt de la Cour (grande chambre) du 13 mai 2014. Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González. Affaire C-131/12.

28. Le renforcement des principes généraux.- Le Règlement européen du 27 avril 2016 reprend les principes déjà contenus dans la directive de 1995 tels que les principes de loyauté, la licéité de la collecte etc. Il affirme également le principe de minimisation, de transparence des données et impose ainsi au responsable du traitement de démontrer et de vérifier la légitimité du traitement des données. Ainsi, le Règlement européen donne une définition plus exhaustive du consentement, notamment en le caractérisant par un acte positif de la personne (article 4, 11°).

Le Règlement prend en compte toutes les formes de traitements et définit notamment la méthode du « profilage » souvent utilisée et qui peut conduire à une atteinte à la vie privée de la personne. L'article 4 4°) du Règlement définit le « profilage », comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ». Cet article répond à la volonté du législateur de veiller à ce que la protection des données soit conforme à la protection de la vie privée visée par l'article 8 de Convention Européenne des Droits de l'Homme (CEDH).

§2- La protection des données à caractère personnel par les droits fondamentaux

Si le considérant n°4 du nouveau Règlement fonde la protection des données sur l'article 8 de la CEDH, la protection des données n'est pas consacrée explicitement par la Convention précitée. Cependant, le Règlement ne manque pas de faire référence à la Charte des Droits Fondamentaux de l'Union Européenne qui consacre la valeur *fondamentale* de la protection des données personnelles, renforçant ainsi l'attention que porte le Règlement au respect de la vie privée[75].

[75] Considérant n°4, du Règlement (UE) 2016/679 op. cit. loci. « *Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent Règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté*

a) L'article 8 de la CEDH et la charte des droits fondamentaux de l'Union Européenne

29. Les données à caractère personnel rattachées à la notion de vie privée.- L'article 8 de la Convention EDH ne fait pas « expressément » référence à la protection des données personnelles. En effet, la CEDH consacre le droit de toute personne au respect de sa « vie privée et familiale ». En revanche, l'article 8 de la Charte des Droit Fondamentaux de l'Union Européenne adoptée le 7 décembre 2000 consacre la protection des données à caractère personnel :

> *« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.*
> *2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.*
> *3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »*

Il est intéressant de remarquer que la Charte des droits fondamentaux de l'UE fait figurer, tout comme la Convention EDH, le droit à la protection des données personnelles à l'article 8. Sans y voir une volonté juridique, cette numérotation peut être considérée comme une heureuse coïncidence pourvoyant ainsi à une meilleure appréciation de la portée de la notion pour le non spécialiste.

30. La protection des données par la Cour EDH.- On peut noter que la protection des données à caractère personnel est précédée par l'article 7 qui consacre le respect de la vie privée et familiale. Ainsi, il ne fait aucun doute que les deux notions sont étroitement liées. Le considérant n°10 de la directive 95/46/CE indiquait déjà que ces deux notions étaient complémentaires. Dix années auparavant, la Cour Européenne des Droits de l'Homme avait affirmé que l'article 8 de la CEDH et la protection des données à caractère personnel issue de la charte relevait du régime de protection du droit à la vie privée. Elle a notamment affirmé que la tenue de fichiers secrets, par la police, contenant des

---

d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique ».

informations sur la vie privée d'une personne, constituait une atteinte, au sens de l'article 8[76]. Elle affirme que cette atteinte est constituée lorsque les informations communiquées n'ont pas été portées à la connaissance de la personne concernée, cette dernière n'ayant pas été mise en position de les réfuter. La Cour a réaffirmé, à plusieurs reprises, le lien entre protection des données personnelles et droit au respect de la vie privée[77]. Concernant des échantillons vocaux, la Cour EDH affirme qu'il y a violation de l'article 8 de la Convention EDH lorsque le prévenu est enregistré dans les locaux d'un commissariat[78] et par conséquent, ces échantillons constituent un détournement de la finalité du système d'enregistrement.

31. La Cour EDH ne s'est pas cantonnée à se prononcer en matière pénale, elle a également affirmé que la notion de vie privée s'appliquait dans le domaine des données de santé à caractère personnel. C'est le cas lorsque ces données sont recueillies par un organisme d'Etat qui effectue une enquête de qualité des soins médicaux, sans avoir recueilli au préalable le consentement de la personne[79]. La question de rattacher la notion de vie privée aux données de santé semble se poser fréquemment. En effet, on peut citer deux requêtes[80] pendantes de la Cour EDH concernant l'accès de l'autorité aux données de santé à caractère personnel. Déjà en 2006[81], la Cour EDH avait condamné la France pour la production de pièces médicales lors d'une procédure de divorce. Dans cette affaire, la Cour EDH avait affirmé que la production de telles pièces, sans le consentement de la personne concernée, constituait une ingérence dans la vie privée de la personne. Elle conclut en motivant sa décision et ajoute qu'en matière de divorce, la même décision aurait été prise sans que ces données ne soient versées au dossier.

---

[76] Cour Européenne des Droits de l'Homme Leander c. Suède du 26 mars 1987, affaire n° 9248/81.
[77] Cour EDH Rotaru contre Roumanie, du 4 mai 2000 sur les fichiers de systèmisation de la mémorisation des informations des services de renseignements et des pouvoirs publics ; Perry c. R-U du 17 juillet 2003 affaire n°35829/97 sur l'usage détourné d'un système de vidéo surveillance durant la garde à vue.
[78] Cour EDH, P.G et J.H. c. Royaume-Uni affaire n° 44787/98.
[79] Cour EDH, L.H. c. Lettonie affaire n° 52019/07 du 29 avril 2014, La requérante alléguait en particulier que la collecte par un organisme d'État (en l'espèce, l'inspection du contrôle de la qualité des soins médicaux et de l'aptitude au travail (MADEKKI)) de ses données médicales personnelles, sans son consentement, avait violé son droit au respect de sa vie privée.
[80] Breyer c. Allemagne (n° 50001/12) Requête communiquée au gouvernement allemand le 21 mars 2016 ; Ćalović c. Monténégro (n° 18667/11) Requête communiquée au gouvernement monténégrin le 31 mars 2016.
[81] Cour EDH, L.L. c. France, requête n° 7508/02, du 10 octobre 2006.

32. La Cour EDH impose de véritables obligations aux Etats et indique que « si l'article 8 tend pour l'essentiel à prémunir l'individu contre des ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'Etat de s'abstenir de pareilles ingérences : à cet engagement plutôt négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée [82]».

On peut enfin remarquer que la Cour EDH est amenée à se prononcer en matière de télécommunication. En effet, la Cour a adressé au gouvernement allemand des questions relatives au respect de l'article 8[83]. Cette requête pendante concerne l'obligation légale pour les opérateurs de télécommunication de conserver les données personnelles de l'ensemble de leurs clients.

On constate, au travers des différentes décisions de la Cour EDH, le rôle fondamental de la protection des données à caractère personnel en matière de protection de la vie privée. En outre, le traité de Lisbonne, entré en vigueur la 1er décembre 2009[84], intègre directement au bloc de constitutionnalité la Charte des Droits Fondamentaux de l'Union européenne, lui conférant ainsi la même valeur juridique que les Traités.

33. La protection des données par la Cour de Justice de l'Union Européenne.- Préalablement, et afin de ne créer aucune confusion, il convient préciser que l'entrée en vigueur du Traité de Lisbonne précité modifie l'ensemble de l'organisation judiciaire de l'Union européenne. Ainsi, la Cour de Justice de la Communauté Européenne (CJCE) est substituée par la Cour de Justice de l'Union Européenne (CJUE) rassemblant la Cour de justice, le Tribunal et le Tribunal de la fonction publique de l'Union européenne.

La CJUE est très prolifique en matière de protection des droits fondamentaux. C'est en s'inspirant des traditions constitutionnelles communes aux Etats membres que la Cour s'assure de la sauvegarde des droits fondamentaux[85]. Elle a été amenée à développer la théorie de « l'effet utile » de la convention dont l'objectif est d'assurer la protection « effective » des droits[86]. En matière de transmission et de conservation de données détenues par les fournisseurs d'accès internet, la Cour affirme que ces opérations relèvent

---

[82] Cour EDH, Odièvre c. France, requête n° 42326/98, du 13 février 2003.
[83] Cour EDH, Breyer c. Allemagne, requête n° 50001/12, du 21 mars 2016 (requête pendante).
[84] Traité de Lisbonne modifiant le traité sur l'Union européenne et le Traité instituant la Communauté européenne, 1er décembre 2009.
[85] J-F Renucci, « Introduction générale à la Convention européenne des Droits de l'Homme Droits garantis et mécanisme de protection », Ed. Conseil de l'Europe, 2005.
[86] CJCE Airey c. Irlande, série affaires n°41, §26, du 9 octobre 1979 ; 13 mai 1980, Artico c. Italie 13 mai 1980.

des questions relatives à la sauvegarde de la vie privée et de la Charte des Droits fondamentaux de l'Union Européenne[87]. Concernant le traitement de données sensibles présentant une violation de la vie privée, l'arrêt *Bodil Lindqvist* indique « qu'une personne qui s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé » au sens de l'article 8, paragraphe 1, de la directive 95/46 ». Selon la Cour, d'après cette directive, il convient de donner une interprétation large de l'expression « données relatives à la santé », employée à l'article 8, paragraphe 1, de sorte qu'elle comprenne « des informations concernant tous les aspects, tant physiques que psychiques de la santé d'une personne ». Il ne fait donc aucun doute que les informations relatives à la santé entrent dans le champ de protection des données. Les informations de santé à caractère personnel relèvent de la « sphère privée », pour reprendre les propos de Monsieur le Professeur Carbonnier. Cette sphère est cependant propice à l'intrusion, notamment avec le développement des TIC. L'information peut être accessible à de nombreux intervenants si la personne concernée n'est pas dûment avisée de son droit de désigner les personnes qui pourront accéder à ses informations. Elle devra également être informée de la marche à suivre pour accéder à ses propres informations ou à son dossier médical.

La protection des données à caractère personnel renvoie donc au respect du principe fondamental du droit à la vie privée consacré par l'article 8 de la Convention Européenne des Droits de l'Homme dont la valeur contraignante est renforcée depuis l'intégration de la Charte des droits fondamentaux de l'Union Européenne au bloc de Constitutionnalité.

La garantie du droit à la vie privée peut se justifier par le fait que chacun est libre de décider de ce qui relève de la sphère privée ou non. En matière de traitement de données à caractère personnel, la détermination de la sphère privée peut se rapprocher du concept d' « autodétermination informationnelle ».

[87] CJCE, Productores de Mùsica de España c. Telefònica de España SAU, affaire C-275/06 du 29 janvier 2008. Dans cette décision la Cour renvoyait aux dispositions de la directive de 1995 et à la directive dite « vie privée et communications électroniques » du Parlement et du Conseil du 12 juillet 2002.

b) Le respect du droit à la vie privée et l'autodétermination informationnelle

34. La notion de vie privée.- La notion de vie privée ne fait pas l'objet d'une définition positive, il convient de tenter de la « définir par la négative », ainsi « la vie privée c'est tout ce qui n'est pas de la vie publique des individus [88]». Ces propos peuvent être complétés par « le droit d'être laissé tranquille » comme le soulignent Samuel D. Warren et L-D. Brandeis[89]. Le critère selon lequel la vie privée serait fondé sur la différence entre les informations qui sont issues de la sphère publique et celles issues de la sphère privée est bien trop réducteur et ne respecterait pas la volonté de la personne. Il convient de se tourner vers le critère du secret fondé sur la volonté de la personne et son droit à l'autodétermination, dégagé par R. Lindon[90].

35. La protection de la vie privée.- L'article 8 de la loi du 6 janvier 1978 modifiée, vise les informations qui ne peuvent pas faire l'objet d'un traitement automatisé. Néanmoins, l'adresse[91], la nationalité, la langue parlée et le lieu de naissance ne sont pas considérés par la CNIL comme des données « sensibles » au sens de l'article 8. Cependant, la pertinence de leur collecte et de leur traitement doit être dûment justifiée, au cas par cas, par le responsable du traitement. Il ressort donc de l'analyse du texte que les données de santé sont des données à caractère personnel et doivent être considérées comme sensibles. Sur le fondement de la protection par le secret, il convient de définir la notion de confidentialité en la distinguant du secret professionnel. Le Code pénal dispose que « la révélation d'une information à caractère secret » par un professionnel, à toute autre personne sans l'accord de la personne, constitue une infraction pénale visée à l'article 226-13 du Code pénal. De même, l'article 1110-4 du Code de santé publique dispose que la violation du principe du respect du secret ouvre un droit à réparation. Le droit au respect du secret est l'extension de l'article 9 du Code civil qui consacre le droit au respect de sa vie privée.

---

[88] R. Badinter, « Le droit au respect de la vie privée », JCP 1968, I n°2136.
[89] « The Right to Privacy », Harvard Law Review, Vol. IV, 1890, p.193-220. Traduit par Françoise Michaut *In* Clio Thémis Revue électronique d'histoire du droit.
[90] R. Lindon, « La presse et la vie privée », JCP 1968, 188, *in* F. Rigaux « La vie privée, une liberté parmi les autres ? », décembre 1992, Larcier.
[91] Il est à préciser que l'adresse figure parmi les informations de la Carte Vitale.

C. Zorn-Macrez[92] fait la distinction entre le respect de la vie privée qui s'impose à chacun et le secret professionnel. En effet, elle relève que l'obligation de confidentialité est une obligation qui astreint chacun d'entre nous, en vertu de l'article 9 du Code civil. Le respect de cette obligation se fonde sur un préjudice subi par la personne concernant sa vie privée dont elle a la maîtrise des frontières. La violation du secret professionnel, en revanche, n'appelle pas forcément un préjudice « pour que l'infraction soit réalisée ».

Selon le Professeur Carbonnier, l'esprit du législateur, dans la rédaction de l'article 9 du Code civil, est de faire respecter une certaine idée de l'intimité de la personne. Il ajoute que la personne, dans sa volonté de se protéger, « aura le pouvoir d'écarter les tiers ». La doctrine traduit cette notion de vie privée par le droit d'être laissé en paix[93], et, plus précisément, « par un devoir d'abstention » des tiers de révéler des informations personnelles. La confidentialité et le secret professionnel seraient donc complémentaires car pour certains auteurs « la confidentialité s'inscrit dans une logique de partage plus étendue que le secret car l'air du temps est à la transparence.[94] ». En effet, J.M Varaut souligne que « la confidentialité permet un transfert d'informations rendu possible parce que son destinataire s'interdit toute communication à des tiers autres que ceux qui sont qualifiés ». L'informatisation massive touchant tous les domaines, il est nécessaire de mettre en balance la garantie du respect des obligations des professionnels et la garantie des droits et des libertés de la personne en consacrant l'effectivité des instruments juridiques tels que l'expression du consentement.

36. Le respect du droit à la vie privée pourrait ainsi être « résumé » par la possibilité de consentir ou non à ce qu'une personne (physique ou morale) puisse avoir accès à une partie de notre personnalité. Cette prérogative s'exprime donc par la volonté de la personne. Par conséquent, la notion de vie privée peut s'analyser à travers la notion de consentement dont le respect est fondamental en matière de traitement de données à caractère personnel et indispensable en matière de traitement de données de santé à caractère personnel.

---

[92] C. Zorn-Macrez. *Données de santé et secret partagé, pour un droit de la personne à la protection de ses données de santé partagées*. Presses universitaires de Nancy, 2010.

[93] Formule également rédigée dans le *privacy Act de 1974* des Etats-Unis d'Amérique.

[94] J.M. Varaut, *«Secret professionnel et confidentialité dans les professions juridiques et judiciaires»,* Gaz. Pal., Rec. 1997, doctr. P. 1054.

37. La portée du consentement.- Malgré les nombreuses lois concernant le commerce électronique, le législateur reste muet quant à la spécificité du consentement. Cela peut être justifié par la volonté de ne pas alourdir les procédures permettant l'expression d'un consentement libre et éclairé. Ce choix[95] peut s'expliquer par la difficulté de mettre en place un formalisme unique qui risquerait de faire entrave à l'innovation. De fait, il semble que le rôle du juge devrait être renforcé afin de permettre la protection des droits, au cas par cas, et l'apparition des caractères communs d'un consentement réel et éclairé. Le rôle du juge sera renforcé dans sa recherche de moyens alternatifs permettant de réaliser une adaptation de la recherche du consentement, notamment en se référant à des moyens extra-légaux à défaut de conditions clairement identifiables[96]. Par exemple, vis-à-vis de l'information que doit délivrer le professionnel de santé afin que le patient puisse consentir, en connaissance de cause, à la collecte et à l'utilisation des données recueillies. Le juge pourra se référer au « guide du professionnel de santé » rédigé par la CNIL[97]. Il pourra également recourir à des chartes, à la doctrine ou à des déclarations[98]. Le Règlement européen invite, dans son article 40, « les États membres, les autorités de contrôle et la Commission » à élaborer des « codes de conduite destinés à contribuer, en fonction de la spécificité des différents secteurs de traitement de données, à la bonne application des dispositions du présent Règlement ». Un consentement effectif et représentatif de la volonté de la personne serait une garantie de plus pour les personnes de tendre au respect de leur droit de « changer [99]».

38. Le principe d'autodétermination dégagé par la Cour Fédérale allemande.- La Cour allemande a dégagé le principe d'autodétermination en le consacrant comme étant le droit de chaque individu de pouvoir se développer librement. La Cour fédérale indique que ce droit à l'autodétermination est une valeur « intermédiaire » qui permet d'éviter la

---

[95] Si c'en est un.

[96] Relativement au consentement électronique, l'une des rares dispositions de nature législative que l'on peut identifier est la directive 2000/31/CE du 8 juin 2000 dont l'art. 10 s'intitulant « informations à fournir » évoque certaines mentions qui sont de nature à éclairer le consentement du consommateur. Antérieurement, la directive européenne du 20 mai 1997 visant à instaurer une meilleure protection des consommateurs au niveau de l'Union européenne peut également être citée.

[97] CNIL- « Le guide du professionnel de santé » 2011 disponible sur http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-guide_professionnels_de_sante.pdf

[98] Conseil National du Numérique « Rapport sur la neutralité des plateformes, Réunir les conditions d'un environnement numérique ouvert et soutenable » Mai 2014.

[99] Décision de la Cour Constitutionnelle allemande arrêt EuGRZ, du 15 décembre 1983.

confusion entre le concept de vie privée et les concepts philosophiques ou politiques[100]. Le troisième attendu de la Cour qualifie les concepts de vie privée et de protection des données personnelles, « d'instruments juridiques nécessaires à la préservation d'une société libre et démocratique ». Ainsi, elle affirme que l'aboutissement d'une société démocratique ne se fait qu'au bénéfice du développement de la personnalité. Les juges de la Cour Constitutionnelle indiquent que la protection des données à caractère personnel ne doit pas s'envisager comme un droit isolé mais comme un droit qui s'exerce dans l'ensemble d'une société libre. Ainsi, la Cour Constitutionnelle allemande affirme que la protection des données à caractère personnel doit être construite de sorte que les systèmes de révélation des données à caractère personnel soient respectueux « du droit de l'individu » à s'autodéterminer. Enfin, la Cour affirme que la raison d'être des régimes de protection des données personnelles, réside dans les rapports asymétriques qu'implique le traitement informatique. En effet, la protection des données vise à équilibrer les pouvoirs entre la personne concernée par le traitement et le responsable du traitement. Certains auteurs remarquent « qu'il n'y a plus de limite quant au volume d'informations pouvant être enregistré » ni de limite quant à « l'étendue de l'analyse pouvant être réalisée [101]».

39. Ce principe dégagé par la Cour Constitutionnelle allemande permet de mettre en lumière les nouveaux procédés de collecte massive des données à caractère personnel. A l'heure du « Big Data », le traitement massif des informations implique un risque de dispersion et de perte de maîtrise des données. Cependant, l'encadrement plein et entier de ces nouvelles formes de collecte et de traitement des données peut se révéler être un atout.

II- Les nouveaux modes de production de données

40. Il est de moins en moins possible de définir à l'avance l'objectif et la nature des données qui seront collectées. La conception contractuelle d'une collecte des données finalisée et proportionnée, comme l'envisage la loi «Informatique et Libertés» de 1978, semble surannée lorsque l'on analyse les nouveaux modes de traitements des données à caractère personnel. Ces nouveaux modes de collecte des données orientent davantage le

[100] Théorie de Westin et Brandeix, op. cit loci.
[101] H. Nissenbaum « Protecting in a Information Age : the problem of Privacy in Public ». NY Univ. Press, 2004, p. 576.

débat juridique sur la question de savoir s'il convient de réguler le traitement des données personnelles en effectuant un contrôle *ex post* prenant en considération les missions et la responsabilité des prestataires techniques lors du traitement des données puisqu'il devient difficile d'effectuer un contrôle *ex ante.*

Beaucoup d'entreprises ont à disposition de nombreuses bases de données dont elles ne sont pas à l'origine de la production. Le mouvement de l'open data vise à favoriser le savoir et la vigilance citoyenne. L'initiative du gouvernement français avec « data.gouv.fr » vise à mettre en place cette vigilance basée sur la participation de chacun. Le site met d'ailleurs en ligne un ensemble de statistiques publiques dans les domaines du logement, de la culture, de l'économie et de l'emploi qui permettent de créer une véritable articulation entre les institutions et les citoyens. Le domaine de la recherche scientifique est l'un des premiers domaines à avoir mis en place de très grandes infrastructures permettant de calculer un grand nombre d'informations.

41. Cependant, il n'existe pas de données que l'on peut qualifier de « brutes » *stricto sensu.* En effet, toute quantification nécessite une construction et est basée sur la recherche d'une partie commune à deux enregistrements. De plus, cette construction est établie par des conventions qui permettent de les interpréter. Plus simplement, en matière de statistiques, il est nécessaire de connaître les catégories de la statistique policière afin de permettre une interprétation de l'enregistrement des mains courantes. L'identification des catégories permet notamment de connaître les effets que produisent les changements de consignes ministérielles sur l'enregistrement des mains courantes. Cependant, sorties de leur contexte et croisées avec d'autres données, ces statistiques risquent de produire un contresens et non une connaissance.

Il convient d'ajouter que ces données ne présentent un intérêt qu'en fonction de la réponse recherchée. En d'autres termes, une donnée a des enjeux multiples. Les données de l'Assurance Maladie sont actuellement utilisées par les administrateurs de l'Assurance Maladie et ont pour fonction de rationnaliser les dépenses. Par exemple, elles permettent de détecter un médecin qui fait de la sur-prescription. Ces mêmes données permettent à des associations de malades de faire apparaître des injustices médicales. En effet, une enquête a permis de démontrer que, de façon implicite, les dialyses étaient davantage prescrites à

des malades de revenus modestes et que les greffes étaient proposées, plus souvent, à des patients dont les revenus étaient plus importants[102].

Si ces données étaient confiées à des compagnies d'assurance, comme il en est de plus en plus question, ces données seraient une véritable mine d'informations. Elles permettraient d'obtenir une véritable prédiction des risques, ce qui serait une véritable contradiction. En outre, on voit se développer, dans le domaine de l'assurance automobile, de plus en plus de traceurs embarqués qui enregistrent des « traces de conduite ». Ces équipements permettent d'enregistrer un comportement et d'en faire une analyse. Cette analyse permettra à l'assureur d'adapter la prime d'assurance, en tenant compte d'un comportement plus ou moins à risques. Or, l'analyse de ces informations n'est que le résultat d'une situation qui a eu lieu à un « instant T » et ne relève pas d'une méthodologie d'interprétation des calculs statistiques.

42. Le fonctionnement des machines statistiques.- Un algorithme n'est véritablement effectif que lorsqu'il parvient à adapter sa méthode de calcul de façon étroite au milieu dans lequel il intervient. C'est le cas du *Page Rank* de Google mais aussi du système de recommandation du site Amazon. De façon plus simple, une situation dans le réel n'est pas « codée », c'est-à-dire que les comportements humains ne relèvent pas de règles que l'on pourrait comparer à celles qui régissent le déplacement de pions sur un plateau d'échec. C'est d'ailleurs pour cela que certains projets d'intelligence artificielle ont échoué car il a été démontré que les machines étaient incapables de s'adapter à l'infinie variété de situations et de contextes[103] propres à l'être humain. Les ingénieurs ont abandonné l'objectif d'un ordinateur ou d'un calculateur doté de concept « ontologiques[104] ». C'est-à-dire qu'ils ont constaté que « la machine » ne pouvait être dotée d'un raisonnement abstrait. En d'autres termes, là où le cerveau est doté d'une capacité d'adaptation, la machine ne peut réaliser que ce que l'algorithme lui permet, dans un contexte qui est préalablement défini. Aujourd'hui, l'enjeu du traitement des données n'est pas une analyse « abstraite » mais l'apprentissage d'un maximum de contextes. C'est-à-dire que l'enjeu n'est plus d'appliquer une grande théorie à un petit volume de données

[102] S. Cabus et P. Santi, « Insuffisance rénale. La parole est aux malades », *Le Monde,* 30 Mars 2013.

[103] H. Dreyfus, *What the Computers Still Can't Do. A Critique of Artificial Reason,* Cambridge, The MIT Press, 1992.

[104] R. Mizoguchi, *Le rôle de l'ingénierie ontologique dans le domaine des EIAH,* STICEF volume 11, 2004.

mais de nombreuses petites théories (calculs) en interrogeant de nombreuses données contextuelles afin d'en sélectionner la ou les meilleures d'entre elles.
Ce qu'il est essentiel de mettre en lumière, c'est que lors du traitement des données il est possible de changer les pondérations affectées aux différentes hypothèses, et ceci en fonction de chaque profil et de chaque contexte d'utilisation. En effet, d'un point de vue purement technologique, les méthodes dites non-paramétriques ont pour avantage de ne pas figer la contribution de leurs variables, mais, bien au contraire, elles ont la « capacité » de réviser constamment leur méthode en fonction des requêtes de l'utilisateur.

Ces méthodes d'apprentissage sont issues des travaux d'ingénieurs en informatique. Les algorithmes sont des méthodes de calcul qui sont commandées par une nécessité commerciale, expérimentale ou logistique. Il serait donc inutile de connaître la composition (technique) d'un algorithme mais il serait beaucoup plus efficace de connaître les flux de données qui « correspondent » à la composition du calcul[105].

43. Il serait décisif[106] de demander aux auteurs des algorithmes de rendre publics les objectifs qu'ils leur confèrent. Cette solution serait en accord avec les dispositions de la loi «Informatique et Libertés» de 1978, mais, également, avec la directive européenne 95/46/CE de 1995 qui impose au maître du traitement de traiter les données de façon loyale, proportionnelle et en accord avec la finalité[107] du traitement informatique. Cette solution se justifie d'autant plus que les modèles « auto-apprenants » sont extrêmement versatiles et que les utilisateurs sont « constamment soumis à des expérimentations massives et sans le savoir [108]».

La démonstration précédente du fonctionnement des algorithmes doit être placée dans le contexte de l'industrie des données. Ces industries ou acteurs commerciaux mettent en place des techniques spécifiques à un secteur commercial et ont pour objectif de valoriser

[105] Le principal objectif qui est demandé à un algorithme est de maximiser l'efficacité d'un service rendu à l'utilisateur, c'est-à-dire qu'il permet de faire une analyse statistique du comportement de l'utilisateur durant sa navigation. L'algorithme définira lui-même la bonne théorie pour que, en chaque situation, les corrélations soient les plus efficaces par rapport à l'objectif visé.
[106] Dominique Cardon, *A quoi rêvent les algorithmes, nos vies à l'heure des big data,* Editions du Seuil et la République des Idées, Octobre 2015.
[107] Cf infra page 101.
[108] D. Cardon, « *A quoi rêvent les algorithmes, nos vies à l'heure des big data »,* Editions du Seuil et la République des Idées, Octobre 2015.

leur activité grâce à l'étude statistique d'informations qu'ils ont décidé d'ordonner selon une organisation précise[109].

44. L'économie des données (enjeux).- A l'origine, la loi «Informatique et Libertés» a été crée par crainte des abus policiers et administratifs. Mais aujourd'hui l'économie est de plus en plus fondée sur la connaissance du « client » et le « capital humain[110] » de sorte que « les données s'achètent, se louent ou se vendent [111]». La montée en puissance de nouveaux dispositifs de suivi et de diagnostic pourrait transformer l'ensemble du système de santé et l'économie en général. La chute des coûts des capteurs et l'articulation des objets connectés avec les terminaux mobiles (smartphones, tablettes, désormais lunettes et les montres connectées) permettent la mise en place de capteurs permanents divers sur des patients afin de suivre leurs activités et détecter les premiers signes de certaines pathologies. Selon une étude de Bloomberg en 2013, les capteurs intégrés devraient passer de 100 millions d'unités en 2014 à 2800 milliards en 2020. Les capteurs pourraient permettre la détection précoce de pathologies et, ainsi, repousser dans le temps la nécessité pour les assureurs d'avoir à prendre en charge, dans la durée, des pathologies lourdes et coûteuses. Le traitement à distance des données des patients n'est pas encore intégré dans l'équation économique de la santé en France, contrairement à de nos voisins britanniques, chez qui les médecins peuvent prescrire des applications mobiles ou des objets connectés dédiés à la santé. Cette évolution n'est que le premier pas vers des transformations beaucoup plus radicales de l'économie de la santé. Le *Nouvel Économiste* résumait ainsi les raisons qui ont, jusqu'ici, prévalu pour expliquer les enjeux liés à aux évolutions de la médecine numérique ainsi qu'aux difficultés de faire évoluer le système de santé en France : « Blocages défensifs, crispations corporatistes, carence de compétences, de management surtout, se conjuguent pour contrarier ces mutations majeures, plus certainement que l'argument traditionnel du manque de ressources financières. Et l'absence d'impulsion politique au plus haut niveau ne fait que rajouter à la difficulté [112]»

---

[109] Loi n° 98-536 du 1er juillet 1998 portant transposition dans le Code de la propriété intellectuelle de la directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données.

[110] G. Desgens-Pasanau, « La protection des données personnelles », 2ème édition, Lextenso, 2012. P. 5 et 147.

[111] Ibidem note préc.

[112] P. Arnoux, « *E-Santé : Les technologies sont là, les mentalités pas encore* », Le Nouvel Economiste, 5 août 2014.

45. La nécessité d'une gouvernance originale des données.- Malgré tout, les informations ne sont pas systématiquement extraites des grandes infrastructures qui créent du volume de données. En effet, les données peuvent être produites par les individus eux-mêmes au travers du « soi mesuré [113]». Cette production est possible grâce à la diffusion des objets communicants. De nombreux mouvements prônent une nouvelle forme de liberté d'expression par le biais du numérique et du chiffrement de la personne[114]. Cette liberté d'expression se fait par la mesure quotidienne. Cette nouvelle forme de mesure devient une sorte de miroir réfléchissant. En effet, le « soi » devient une unité à laquelle on se mesure, dans un but permanant de s'améliorer. Activités sportives, déplacements, temps de sommeil, signaux corporels, actes sexuel, etc. Certains auteurs qualifient ce comportement de *« benchmark personnel [115]».* Outre que cette utilisation peut servir à savoir si « on » « agit bien », il s'agit de prendre conscience que ces enregistrement personnels visent à créer un écosystème agrégeant un flux de données, pouvant être partagées avec d'autres utilisateurs, mais aussi mises en corrélation avec d'autres bases de données plus riches. De plus en plus d'objets connectés qui se trouvent autour de *nous* deviennent actifs dans notre quotidien et sont de plus en plus performants dans leurs rétroactions avec l'utilisateur. Ces systèmes ouvrent de nombreuses possibilités mais le flux de données et d'informations qu'ils génèrent posent la question quant à la gouvernance de ces nouvelles données.

46. La patrimonialité des données ?- Deux possibilités peuvent être proposées en l'espèce : soit l'utilisateur confie l'enregistrement de ses informations personnelles à des services qui les croisent, il perd alors le contrôle de ses données personnelles ; soit l'utilisateur devient l'administrateur de ses données et interprète lui-même ses informations en faisant lui-même le croisement. Ces deux situations réclament une gouvernance et un encadrement juridique original. Cela permettrait de profiter des savoirs que ces informations permettent[116]. Cette nouvelle gouvernance devra s'effectuer « sans favoriser

---

[113] Traduit littéralement de l'anglais « *Quantified self*».

[114] Les Cahiers de la CNIL, *Quantified self, m-santé : le corps est il un nouvel objet connecté ?,* 28 mai 2014.

[115] A-S. Pharabod, « *La mise en chiffre de soi. Une approche compréhensive des mesures personnelles* », Réseaux, n°177, 2013.

[116]« Les plus beaux projets Big Data se trouvent pourtant dans des secteurs que l'on observe moins, mais qui nous concernent tout autant. Logistique, maintenance prédictive, recherche, santé, énergie, culture et humanitaire même » Guide du Big Data, « *l'annuaire de référence à destination de l'utilisateur »,* 2014/2015.

des phénomènes de centralisation et sans menacer la vie privée des personnes [117]». Certaines affaires ont démontré qu'il suffisait de très peu d'informations pour désanonymiser, par recoupement, des bases de données qui paraissaient, en apparence, bien sécurisées[118].

A l'heure où un volume important de données personnelles est produit et traité, il serait impossible de connaître à l'avance le sens et la nature des calculs qui vont être conduits à partir des données collectées. La transparence des moyens de traitement est, en principe, assurée par l'obligation de définir la finalité du traitement envisagé. La transparence apparaît comme une *conséquence* due à l'appariation de nouveaux acteurs nommés « data brokers », que l'on peut traduire par « courtiers de données[119] », dont la « mission » est de *sonder* et valoriser les données. C'est le « Data meaning ».

47. Le Data meaning.- Le data meaning ou le « profilage » recouvre une nouvelle manière de traiter les données. Le procédé du profilage est construit sur l'accumulation des données recouvrant tous les domaines. Cette accumulation permet ensuite d'effectuer un « forage » dont le résultat permet de reconstituer une tendance ou un comportement. Ce procédé peut être illustré par l'exemple des réseaux sociaux où nos comportements sont « sondés », le plus souvent à notre insu. Ces nouveaux modes d'interprétation des données et de collecte n'ont pas pour résultat le reflet numérisé d'un individu autonome. Le profilage est une technique de surveillance ou d'exploitation des données qui permet, sur « la base de profils établis », d'effectuer une mesure de la personne et d'en dégager une décision[120].

48. Une évolution souhaitable de la protection des données personnelles ?- La gouvernance des données à caractère personnel et des données de santé implique la nécessité d'un encadrement légal de l'utilisation de ces dernières afin d'éviter des dérives commerciales ou une rupture d'égalité en termes d'accès aux soins, à la sécurité sociale, à

---

[117] Dominique Cardon, A quoi rêvent les algorithmes, « *Nos Vies à L'heure des Big Data »,* Edition Seuil, La République des Idées, Octobre 2015.

[118] En avril 2016, plus de 50 millions de données personnelles ont été dévoilées et mises en circulation, exposant les personnes concernées à diverses fraudes, http://www.cil.cnrs.fr/CIL/spip.php?article2851.

[119] « Data brokers : aux Etats- Unis, votre vie privée est en vente », ZDNet.fr, 12 avril 2013, http://www.zdnet.fr/actualites/data-brokers-aux-etats-unis-votre-vie-privee-est-en-vente-39789295.html.

[120] Voir à ce sujet J. Ph. Walter, « Le profilage des individus à l'heure du cyberespace : un défi pour le respect du droit à la protection des données. Disponible sur www.crid.com

un emploi, à une assurance ou à un crédit. L'objectif de l'utilisation des données de santé est d'assurer la qualité des soins tout en préservant les libertés fondamentales telles que la vie privée et la confidentialité.

La difficulté provient de la multiplicité des informations mais, aussi, de leurs enjeux en termes économiques, sanitaires et démocratiques. En d'autres termes, l'utilisation des bases de données constituées à partir de données de santé individuelles, à des fins collectives d'étude ou de recherche, ne doit pas venir compromettre le droit de chacun au respect de sa vie privée.

De manière générale, les données à caractère personnel sont dites sensibles car elles permettent de comprendre ou d'identifier un comportement, d'établir un mode de vie, de définir des goûts ou des besoins pour une personne ou un groupe de personnes. Dès lors, il serait facile pour une entreprise commerciale ou une société de crédits, de savoir quels types de stimuli ou d'informations pourraient être « injectés » dans le quotidien d'un individu afin qu'il puisse augmenter sa consommation. De même, un assureur pourrait directement, sans que cela lui soit communiqué par l'assuré, savoir quelle prime d'assurance imposer à l'assuré ayant une maladie cardiaque, neurologique ou atteint de diabète.

49. Ces informations regroupées sur une base de données sont susceptibles d'aboutir à des atteintes aux droits fondamentaux, et, plus généralement, aux droits de la « personnalité[121]». « Big Brother » n'est plus aujourd'hui un fantasme mais bien une réalité. Il est devenu un moyen spécifique de contrôle du traitement des informations collectées via l'informatique. Néanmoins, un partage trop large des informations pourrait compromettre le respect des libertés individuelles. Il apparaît nécessaire de trouver un équilibre entre l'échange d'informations utiles à la pratique médicale et le respect de la vie privée. Il est opportun de se demander quelle est la finalité de l'information partagée à tous les niveaux (épidémiologie, recherche etc.).

Vis-à-vis du patient, quels types d'informations seront jugées nécessaires à sa prise en charge et bénéfiques en termes de soin ? Seront-elles toujours utilisées « dans un but strictement thérapeutique » ? Pour reprendre les termes du Code de santé publique. Où se trouve la frontière entre le caractère personnel de l'information et le caractère médical ?

---

[121] F. Terré, D. Fenouillet, *« Droit civil. Les personnes. »* Dalloz coll. Précis, 8ième édition, octobre 2012 p59.

La multiplicité des outils informatiques, à but professionnel ou personnel – comme les applications de santé - permet un partage quasi illimité des données de santé et appelle à une sensibilisation des professionnels de santé, du patient mais aussi du client d'une officine. « Le traitement des données »[122] de santé partagées doit alors s'analyser au regard des règles de la législation «Informatique et Libertés», mais, également « au jour d'un foisonnement vertigineux de normes relatives à la mise en œuvre de dossiers spécifiques comme le Dossier Médical Personnel, le Dossier Pharmaceutique ou l'historique des remboursements [123]». L'objet de cette étude est de savoir, en l'état actuel du droit, ce que représente et contient une donnée de santé afin de faire une analyse des éléments techniques permettant de la traiter informatiquement, dans le respect des droits fondamentaux, de la déontologie médicale, du droit à la vie privée et du secret médical afin d'en tirer l'éventuelle nécessité de lui consacrer un régime spécifique.

50. L'évolution fulgurante des technologies informatiques peut constituer un danger pour la protection des données de santé. Ces dernières peuvent se voir perdues, corrompues, détruites voire détournées. Ainsi, le récent cas de suicide du prévenu suspecté d'avoir volé le dossier médical de Michael Schumacher[124] rappelle que les données médicales, du fait de leur caractère éminemment personnel, restent des données sensibles devant faire l'objet d'une protection particulière. La France est pionnière en la matière puisqu'elle dispose d'un régime juridique protégeant l'ensemble des données personnelles. Ce régime date de la loi du 6 janvier 1978. L'objectif principal de cette loi est d'assurer la sécurité du traitement des données à caractère personnel. Parmi ces dernières, on trouve les données médicales qui font également l'objet de dispositions particulières. En effet, le législateur a jugé que ces données, sensibles par nature, nécessitaient une protection spécifique. Ainsi, le Code de la santé publique protège les données médicales et leur traitement par les professionnels de santé.

Néanmoins, cette protection ne s'impose qu'à une catégorie de professionnels soumise aux obligations spécifiques inhérentes à leur titre. C'est alors que se pose la question de savoir si les éditeurs d'applications de santé sont soumis aux règles de secret médical ?

---

[122] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[123] Arrêté du 14 mars 2007 relatif aux spécifications physiques et logiques de la carte d'assurance maladie et aux données contenues dans cette carte, JORF n°65 du 17 mars 2007 page 4983.
[124] « Vol du dossier médical de Schumacher : un suspect se pend en prison », le *Monde,* 6 août 2014.

Une donnée informatique est, par définition, immatérielle. Elle suppose donc une localisation sur un serveur. Par exemple, dans le cas où un ressortissant français tomberait malade dans un pays étranger et serait soigné sur-place, ses données de santé à caractère personnel ne seraient pas situées sur le territoire national. La loi française ne s'appliquant que sur le territoire français, le régime de protection des données médicales pourra se voir alors modifié et certaines atteintes à la confidentialité des données de santé, seraient peut-être tolérées alors qu'elles constitueraient une infraction pour le droit français.

Dès lors, quelle est la réelle portée juridique de la protection des données de santé à la fois au plan national et international ? L'évolution récente de certaines technologies informatiques peut-elle entrer en contradiction avec la confidentialité de ces données dites sensibles?

Les données personnelles sont omniprésentes sur internet et leur importance économique est croissante. Pour les services de la société de l'information tels que les moteurs de recherche, les réseaux sociaux ou les sites de vente en ligne, elles sont devenues indispensables. Ces services, apparaissant comme essentiellement gratuits pour les utilisateurs, ont en réalité un modèle économique particulier : la monétisation des données personnelles des utilisateurs en échange d'un accès gratuit. Le texte originel du 6 janvier 1978 «Informatique et Libertés» est le texte de référence en matière de protection des données à caractère personnel.

Les modifications du texte de 1978 ont permis, non-seulement une protection élargie des données à caractère personnel, mais également de fonder un droit à l'autodétermination informationnelle et d'assurer la garantie d'un traitement des données dans le respect du droit à la vie privée (Partie 1).

51. Cependant, la loi dite «Informatique et Libertés» ne prenait pas en compte l'apparition de nouveaux traitements de données sensibles, en dehors du domaine médical.

La directive Européenne 95/46/CE a fait un apport en la matière. C'est le rapport Braibant de 1998 qui a affirmé que les données biométriques et génétiques étaient des « *données différentes* » qui font l'objet de traitements de façon très courante. La transposition de la directive 95/46/CE par la loi du 6 août 2004 a permis d'introduire une protection spécifique vis-à-vis du traitement des données biométriques et génétiques.

Cependant, on assiste au développement de nouvelles technologies qui permettent la collecte d'un nouveau type de données personnelles qui se rattachent à une personne, qui permettent son identification, et qui sortent du cadre réglementé du cabinet médical. Les

nouvelles technologies de l'information font apparaître un nouveau type de données qui est difficile à définir[125]. Ces nouveaux types d'informations sur la santé générés et collectés directement par la personne concernée par le traitement font également l'objet de nombreux travaux au niveau européen. En effet, le Parlement Européen et le Conseil de l'Europe ont adopté un Règlement visant à renforcer le cadre juridique en matière de circulation et de protection des données à caractère personnel. Le renforcement de la protection des données personnelles et des données de santé fait également l'objet d'un projet de loi par la secrétaire au gouvernement A. Lemaire qui vise à développer une « république numérique » permettant le renforcement de certains principes fondamentaux comme le droit d'accès ou le droit à l'information.

Le projet de loi développe de nouveaux concepts comme « l'habeas corpus numérique » qui vise à renforcer les prérogatives de chaque utilisateur en lui permettant une plus grande maîtrise de ses données personnelles, notamment dans le domaine des données de santé (Partie 2).

[125] J.-M. Job, « la loi Informatique et Libertés » et les données de santé », RLDI 2008/34 n°1161

Partie 1 : La protection des données personnelles fondée sur le principe d'autodétermination

Il convient d'étudier les différentes notions relatives à la protection des données à caractère personnel. En effet, il s'agit d'analyser ce que recouvrent les notions de *traitement* et de *données à caractère personnel* (Titre 1) pour enfin étudier le régime d'application de la protection, dont l'objectif est de garantir la neutralité de la collecte et du traitement des données à caractère personnel (Titre 2).

Titre 1 : La Présentation des données à caractère personnel et de la notion de traitement

La notion de « donnée à caractère personnel », et, plus précisément, les contours permettant de la définir, ont fait l'objet d'extension dans sa définition légale. En effet, la notion de donnée à caractère personnel a succédé au terme « *d'information nominative* ». Elle a également fait l'objet de nombreuses interprétations. La notion de donnée à caractère personnel fait référence, d'une part, aux informations permettant d'identifier directement ou indirectement une personne physique, et, d'autre part, aux données qui permettent de faire référence à une personne physique par déduction notamment par le recoupement d'informations sensibles. Le caractère personnel recouvre également les données pour lesquelles le processus d'anonymisation a été insuffisant, lacune qui pourrait permettre une ré-identification de la personne par croisement des données. L'extension de la définition de données à caractère personnel tient compte des nouveaux modes de traitements algorithmiques, notamment les traitements concernant l'identité numérique. Il convient d'analyser le champ d'application matériel de la loi afin de définir ce que recouvre la notion de traitement des donnée à caractère personnel (chapitre 1) afin de dresser les différentes typologies de données à caractère personnel (chapitre 2).

Chapitre 1 : Définition et analyse du traitement des données à caractère personnel

L'analyse du champ d'application matériel de la protection des données à caractère personnel fait référence aux différentes notions contenues dans les textes. Il conviendra de définir la notion de traitement (section 1) afin de mettre en évidence les critères permettant la qualification de *données à caractère personnel* (section 2).

Section 1 : La notion de traitement

La notion de *traitement* des données à caractère personnel renvoie à la notion de *moyens* de traitement. C'est-à-dire qu'il convient de savoir comment sont organisées et manipulées les données. On peut scinder les moyens de traitement en deux : les moyens de traitement automatisé (§1) et les moyens non automatisés (§2).

§1- Traitement automatisé

Il convient d'étudier les origines et l'évolution de la notion de traitement automatisé(a) afin de dégager les critères qui permettent l'interprétation et l'application de la notion(b).

a) Origine et évolution de la notion de traitement automatisé

52. L'article 2 de la loi «Informatique et Libertés» définit le traitement de données comme « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et, notamment, la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, [et] l'effacement »[126]. La succession de termes démontre la volonté du législateur d'intégrer un maximum d'éléments dans le champ d'application de la notion de traitement informatique des données. Cette accumulation de termes ne permet pas pour autant son assimilation dans le

[126] R. Perray, « Données à caractère personnel, introduction générale et champ d'application de la loi « Informatique et Libertés », J.Cl Comm, fasc, 4710, 2014, spéc. n°25 et s.

langage informatique[127]. En d'autres termes, la notion de traitement « *automatisé* » n'est pas clairement définie. Le législateur ne fait référence qu'à une somme d'opérations mettant en place une organisation de l'information collectée. La directive européenne 95/46/CE ne définit pas non plus le terme « automatisé ».

Le terme de traitement « automatisé » trouve son origine dans le rapport TRICOT[128] dont le législateur français s'est ispiré. Le terme « automatisé » apparaît dans les débats et les rédacteurs du rapport souhaitaient d'ailleurs que la fonction « automatisée » ne soit pas limitée à l'informatique[129]. La Commission Nationale de Informatique et des Libertés (CNIL), dans son premier rapport annuel d'activité, adoptait une définition fonctionnelle en indiquant que « la notion de traitement ou d'application correspondant, par conséquent, à l'ensemble des informations et des logiciels qui concourent à la mise en œuvre d'une fonction principale donnée ; cette interprétation tient compte du fait qu'une même application informatique peut faire appel à plusieurs fichiers[130] ».

53. La directive européenne 95/46/CE définit la notion du traitement automatisé aux articles 2 et 3 et dispose que le texte s'applique aux traitements qu'ils soient automatisés ou non. On remarque que dans le texte la définition est très extensive alors qu'antérieurement la convention 108 du 28 janvier 1981 du Conseil de l'Europe retenait une conception plus restrictive[131]. Compte tenu de l'évolution des technologies, le législateur européen a souhaité conserver une certaine neutralité dans la définition afin qu'elle puisse être adaptée à toutes les évolutions de traitements.

---

[127] A. Lucas, J. Devèze et J. Frayssinet, « *Droit de l'informatique et de l'internet* », Puf, coll, Thémis droit privé, 2001.

[128] Rapport remis le 27 juin 1975 par le biais de Bernard Tricot. Projet de loi élaboré sur la base de ce rapport a abouti à l'adoption de la loi du 6 janvier 1978 sur l'informatique, les fichiers et les libertés. Tricot, Bernard. Rapport de la Commission Informatique et Libertés: (décret 74-938 du 8 novembre 1974).Paris: La Documentation française, 1975. Volume 1. p. 7.

[129] Rapport de la Commission Informatique et Libertés, La Doc. Fr., Coll, rapports officiels, 1975, spéc. p.8 et 21.

[130] CNIL, Rapport annuel, la Doc. Fr., coll, rapports officiels, 1979, p.25. La CNIL fait une confusion en assimilant le fait qu'il ne peut y avoir traitement sans fichier alors que, nous l'avons vu dans l'introduction, il peut y avoir traitement sans fichier. La CNIL faisait une analyse contextuelle de la problématique du traitement car les TIC n'étaient pas aussi développés.

[131] Convention STE n°108 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981. Dans son article 2, la Convention définit le traitement et exclut la collecte. Voir le rapport explicatif §31 disponible sur http://www.coe.int/fr.

54. En droit interne, la directive 95/46/CE a fait l'objet d'une transposition par la promulgation de la loi n° 2004-801 du 6 août 2004[132]. Lors de la transposition de cette directive, le législateur français a repris la définition posée par la directive européenne mais il a souhaité préciser et élargir le champ d'application matériel de la nouvelle définition, en précisant que la qualification de traitement doit être retenue « quel que soit le procédé utilisé »[133]. Il convient de noter que cet élargissement avait déjà été proposé par la CNIL dans son avis du 26 septembre 2000[134].

Si l'on compare[135] la loi de 1978 et celle de 2004, on constate que la loi «Informatique et Libertés» limitait la notion de traitement à « un ensemble d'opérations relatif à la collecte (…) ainsi que tout ensemble d'opération de même nature se rapportant à l'exploitation de fichiers ou de bases de données et notamment les interconnexions (…) ». La loi de 2004 reprend la directive 95/46/CE et retient que la notion de traitement s'applique à « toutes opérations ou ensemble d'opérations ». Dès lors, une seule des opérations définies par la loi suffit à qualifier le traitement automatisé des données personnelles, alors que la combinaison de deux opérations était nécessaire, auparavant, pour emporter la qualification de traitement automatisé[136]. Il convient de remarquer que la liste des opérations de traitement a été élargie. En effet, la loi ajoute à la liste des opérations de traitement « l'organisation, l'adaptation, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage et l'effacement[137] ».

55. Avant d'étudier l'application et les différentes interprétations de la notion de traitement automatisé par les différentes autorités, il convient de préciser que le règlement européen présenté par la Commission Européenne le 25 janvier 2012 et adopté le 14 avril

---

[132] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004 page 14063.

[133] Loi du 6 août 2004 op.cit.

[134] CNIL, Rapport annuel, la Doc.fr., coll, rapports public, 2000, p.17 à 19. Dans son avis, la CNIL encourageait le gouvernement à appliquer la loi « quel que soit le dispositif employé ».

[135] G. Desgens-Pasanau, « La protection des données personnelles », 2ème édition, Lextenso, 2012. P 8; C. Castet-Renard, « Droit de l'internet ; Droit français et européen », Montchrestien, éd. Lextenso, 2012, p42.

[136] TGI de Paris, 5 décembre 1991, *Expertises* 1992, p.107, note de J. Frayssinet. Le TGI de Paris a considéré que le traitement n'était constitué que s'il y avait collecte et enregistrement.

[137] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004 page 14063.

2016 reprend la définition de la directive 95/46/CE[138]. Cependant, il serait nécessaire d'ouvrir les débats au sujet de la notion de traitement, et ceci en raison des nouveaux paramètres à prendre en considération avec le développement d'internet. En effet, comme abordé dans l'introduction, les nouveaux gisements de données et les opérations de calcul en amont du traitement permettent de mettre en place des algorithmes. Ces algorithmes vont au-delà de la définition prévue par la directive 95/46/CE car ils permettent, non seulement un traitement automatisé en fonction de la pondération qu'il leur a été affectée, et une adaptation de leur *réponse* en fonction du comportement de l'utilisateur. En revanche, il semble que la Commission ait voulu élargir la définition de données à caractère personnel, ce qui, compte tenu du nombre de données traitées, semble être le plus urgent afin de garantir la protection des personnes.

b) L'application et l'interprétation de la notion de traitement automatisé

56. La Cour de Justice de l'Union Européenne (CJUE) effectue une interprétation large de la notion de traitement des données à caractère personnel[139]. L'arrêt *Bodil Lindqvist* affirme que « l'opération consistant à faire référence, sur une page internet, à diverses personnes, et à les identifier, soit par leur nom, soit par d'autres moyens, par exemple par leur numéro de téléphone ou d'autres informations constitue un traitement au sens de l'article 3 §1 de la directive 95/46/CE[140]. De même, dans l'arrêt CJCE du 16 décembre 2008, la Cour affirme que l'activité « consistant à collecter des données personnelles dans des documents publics, à les publier en les structurant, à les céder sous la forme de CD-Rom et à les traiter sous la forme de service SMS […] » constitue un traitement de données à caractère personnel[141]. Récemment, la Cour s'est prononcée sur le cas des données traitées et produites par un moteur de recherche. Le 13 mai 2014, dans l'affaire *Google Spain*, la CUJE affirme que le fait d'extraire, enregistrer, organiser, conserver, communiquer et mettre à disposition des informations autres que celles relatives aux données personnelles et ayant déjà fait l'objet de publications, constituaient des

[138] Règlement du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) COM (2012), 11, final, 2012/0011 (COD).
[139] R.Perray, « *Informatique, Introduction générale et champ d'application de la loi « Informatique et Libertés »,* J.Cl. Comm, fasc 274-10, mai 2016.
[140] CJCE, 6 novembre 2003, affaire C-101/01, *Bodil Lindqvist,* §27.
[141] CJCE, 16 décembre 2008, affaire C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy,* §37 ; *Europe* 2009, comm. 54, observations E. Bernard.

opérations de traitement automatisé des données à caractère personnel[142]. Enfin, dans l'affaire *Bavarian Lager*[143], la Cour de justice a repris la définition de traitement de données à caractère personnel de la directive européenne 95/46/CE en affirmant qu'une seule opération énumérée dans la définition suffisait à constituer un traitement, et ce même lorsque la communication d'informations à des tiers est ponctuelle. Cette interprétation large de la part de la Cour de Justice de l'Union Européenne va dans le sens de la CNIL.

57. L'interprétation extensive de la CNIL.- Concernant l'interprétation de la notion de traitement automatisé, la CNIL a toujours eu une vision large[144] de son champ d'application. La CNIL affirme qu'il y a traitement de données à caractère personnel dès que le moyen utilisé est automatisé. En effet, elle considère que la collecte[145], la visualisation[146] ou le simple tri emporte la qualification de traitement automatisé des données à caractère personnel.

Dans le même sens, l'Autorité Administrative Indépendante considère que la recherche et le recoupement de fichiers[147], la normalisation et l'enrichissement des données[148] constituent un traitement automatisé des données. Elle va même jusqu'à affirmer que le processus d'anonymisation[149] est un moyen automatisé de traitement des données à caractère personnel.

En ce qui concerne les moyens *automatisés*, la CNIL interprète le texte de façon large et affirme, dans sa délibération du 18 septembre 1984, que la mise en place d'un autocommutateur téléphonique correspond à un moyen automatisé de traitement[150]. De

---

[142] CJUE ; 13 mai 2014, affaire C-131/12, *Google Spain SL, Google Inc, C. Agencia Española de Protecciòn de Datos, Mario Costeja Gonzalez, spéc. §28 ; JCP E 2014, 1326,* note de M. Griguer et 1327, note G. Busseuil ; A.Debet « *Google spain : Un droit l'oubli ou oubli du droit ? »,* Comm. Com. Electr. 2014, legalis.net.

[143] C-28/08 P Commission c/ Bavarian Lager, arrêt du 29 juin 2010.

[144] V.R. Perray, « *Les données à caractère personnel, Introduction générale et champ d'application de la loi « Informatique et Libertés* », J.-Cl. Comm., fasc. 4710, 2014, spéc, n°41.

[145] CNIL, délibération n°80-34, relative au traitement automatisé de la comptabilité générale, du 21 octobre 1980.

[146] CNIL, délibération n°86-13, portant dénonciation au Parquet de Paris d'infraction à la loi du 6 janvier 1978, 14 janvier 1986.

[147] CNIL, délibération n°2011-418, portant avis sur un projet de décret relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle, 15 décembre 2011.

[148] CNIL, délibération n°2012-209, portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs la gestion de clients et de prospects, 21 juin 2012.

[149] CNIL, « La sécurité des données personnelles », Coll. Guide. Edition 2010.

[150] CNIL, Délibération n°84-31, du 18 septembre 1984, portant adoption d'une recommandation concernant l'usage des autocommutateurs téléphoniques sur les lieux de travail.

même, la position de la CNIL est stricte en matière de surveillance des personnes : s'agissant du traitement de l'adresse IP, la CNIL affirme que la collecte de l'adresse IP constitue un traitement car l'autorité administrative qualifie l'adresse IP de donnée à caractère personnel. Cependant, à propos des contrefaçons sur internet, elle indique que le fait de mettre en place un système de recherche, même ponctuel, sur internet, afin de permettre l'appréhension d'auteurs de contrefaçons audiovisuelles, ne constitue pas un traitement automatisé des données à caractère personnel. Il semble que la CNIL fasse une application au cas par cas et affirme son pouvoir en matière d'autorisation préalable au vu de la délibération du 21 décembre 2006 qui a autorisé l'Association de Lutte contre la Piraterie Audiovisuelle à effectuer un traitement des données personnelles ayant pour finalité principale la recherche d'auteurs de contrefaçons audiovisuelles[151].

58. Jurisprudence interne, une interprétation stricte du traitement.- La jurisprudence interne en matière d'interprétation de la notion de traitement à interprétation se montre stricte que cela soit avant ou après la transposition de la directive européenne de 2004[152]. L'interprétation stricte en matière de traitement automatisé se révèle notamment en matière pénale et peut s'expliquer par la volonté du juge de vouloir appliquer les principes du droit pénal. Cette interprétation en matière pénale se justifie également par le souhait de ne pas voir annulée une décision pour non respect de l'application de la loi «Informatique et Libertés». De plus, la Cour de Cassation a affirmé, dans son arrêt du 16 mars 2004, que le fait de saisir des informations à l'aide d'un ordinateur afin de les imprimer ne constituait pas un traitement, qualifiant ainsi de machine à écrire l'ordinateur ayant servi à la saisie des informations[153].

59. La preuve de l'existence du traitement.- Le traitement automatisé des données à caractère personnel doit faire l'objet d'une déclaration préalable[154] auprès de la CNIL. La mission de la Commission sera de délibérer sur la licéité du traitement envisagé. Cependant, au vu de la jurisprudence en la matière, il semble complexe de rapporter la preuve du traitement. En effet, la Cour de Cassation indique qu'il n'y a pas la preuve d'un

[151] CNIL, délibération n°2006-294 du 21 décembre 2006.
[152] A. Debet, « *Le champ d'application matériel de la notion de traitement des données à caractère personnel »,* La protection des données à caractère personnel en droit Français et Européen, ed, Lextenso, 2015.
[153] Cass. Crim. 16 mars 2004, inédit, n°04-80048.
[154] Cf infra, Titre 2 La neutralité de la collecte des données comme fondement de la protection des données de santé à caractère personnel p100.

traitement automatisé lorsqu'une société a pour projet l'évaluation des salariés via l'analyse des données personnelles recueillies au cours d'entretiens individuels, même à défaut de déclaration préalable auprès de la CNIL.

En effet, la personne concernée (le requérant) devra prouver qu'il y a un défaut de déclaration préalable auprès de la Commission mais il devra également prouver que ses informations ont fait l'objet d'un traitement automatisé[155]. Néanmoins, la Cour de Cassation a évolué dans son acception du traitement, notamment en matière de droit du travail et de droit commercial. En effet, la Cour a affirmé que les fichiers client, en l'absence de toute déclaration préalable, doivent être considérés comme illégaux sur le fondement de l'article 1128 du Code civil et de l'article 22 de la LIL du 6 janvier 1978[156]. Enfin, suite à son licenciement pour abus d'utilisation de la messagerie interne de l'entreprise, la requérante a saisi la cour d'Appel d'Amiens[157] qui confirme la cause réelle et sérieuse du licenciement en appuyant sa décision sur les preuves issues du dispositif de contrôle individuel de l'entreprise n'ayant pas fait l'objet d'autorisation de la CNIL.

60. Charge de la preuve, position de la Cour de Cassation.- Le 8 octobre 2014 la chambre sociale de la Cour de Cassation affirme que *« constituent un moyen de preuve illicite les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la CNIL ; Qu'en statuant comme elle l'a fait, en se fondant uniquement sur des éléments de preuve obtenus à l'aide d'un système de traitement automatisé d'informations personnelles avant qu'il ne soit déclaré à la CNIL, alors que l'illicéité d'un moyen de preuve doit entraîner son rejet des débats, la cour d'appel a violé les textes susvisés».* Ainsi la Cour de Cassation affirme que les preuves

[155] Cass. Com. 28 novembre 2007, n°06-21964, publié au bulletin, JCP E 2008, n°13, obs, M. Vivant, N. Mallet-Poujol et J-M Bruguière.

[156] La Cour de cassation a tiré des conséquences inédites et radicales de l'absence de déclaration d'un traitement, dans une affaire de vente de fichiers de clientèles. Apprenant que le fichier de clients transmis (et ne tenant pas toutes ses promesses commerciales !) n'avait pas été déclaré à la CNIL, l'acquéreur avait assigné le vendeur en nullité de la vente. La Cour d'Appel avait rejeté cette demande en considérant que la loi n'avait pas prévu que l'absence d'une telle déclaration soit sanctionnée par la nullité. L'arrêt a été cassé – au double visa des articles 1128 du Code civil et 22 de la loi du 6 janvier 1978 – au motif, relativement lapidaire, que « tout fichier informatisé contenant des données à caractère personnel doit faire l'objet d'une déclaration auprès de la CNIL » et que la vente d'un tel fichier qui, « n'ayant pas été déclaré, n'était pas dans le commerce », avait un « objet illicite » (Cass. com., 25 juin 2013, no 12-17.037, Com. com. électr. 2013, no 9, comm. 90, note Loiseau G., D. 2013, p. 1867, note Beaussonie G., JCP G 2013. 930, p. 1619, note Debet. A., RLDI 2013/96, no 3188, note Varet E. et no 3189, note Mendoza-Caminade A., RLDI 2013/97, no 3222, note Perray R., RLDI 2013/98, no 3248, note Soubelet-Caroit S. et Soubelet L. et no 3264, note Naftalski F. et Colas-Bernie A.-C.).

[157] CA, Amiens, 29 janvier 2013, n°1314911 ; Cass. Soc. 8 octobre 2014, n°1738.

tirées d'un moyen de traitement automatisé, hors autorisation préalable de la CNIL, doivent être écartées des débats, et ce, même lorsque l'autorisation est accordée postérieurement aux faits[158].

Des difficultés similaires se retrouvent dans le traitement de données à caractère personnel mettant en œuvre des moyens non automatisés de traitement. Ni la loi «Informatique et Libertés», ni la directive européenne 95/46/CE ne font la différence entre ces deux moyens. Il semble néanmoins nécessaire d'en préciser les contours.

§2- Le traitement non automatisé

La loi «Informatique et Libertés» ainsi que la directive européenne 95/46/CE ne font pas de différence entre les traitements automatisés et non automatisés. Cette volonté de la part du législateur vient du fait que seuls les traitements non automatisés contenus dans un fichier sont soumis à l'application de la loi «Informatique et Libertés» d'une part (a) et, d'autre part, certaines dispositions de la même loi ne sont pas applicables aux traitements manuels (b) même lorsqu'ils sont contenus dans un fichier ; c'est le cas des copie temporaire (c)

a) La notion de traitement non automatisé dans un fichier

61. L'article 2 de la loi «Informatique et Libertés» dispose que le texte « *s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenus ou appelés à figurer dans des fichiers »* et ajoute que les fichiers de données se définissent « *comme tout ensemble structuré et stable de données à caractère personnel accessible selon des critères déterminés ».* Donc, les traitements non automatisés de données sont soumis aux mêmes règles que le traitement automatisé. Initialement, la loi «Informatique et Libertés» avait été construite dans le but de protéger du traitement les données « nominatives [159]». La loi

[158] Cass. soc., 8 octobre 2014 , n°13-14991, publié au bulletin numérique des Chambres civiles, (ECLI:FR:CCASS:2014:SO01738). Note A. Laconste.
[159] Voir les articles 1 à 44 de la loi «Informatique et Libertés» du 6 janvier 1978 et les travaux préparatoires du Rapport TRICOT cité précédemment note 3.

intégrait également dans son article 45 la notion de *fichiers* et de *traitements* non automatisés.

La CNIL avait défini, à l'origine, le fichier comme « une collection d'entités homogènes décrites par des éléments d'information […] une collection de données pouvant indifféremment porter sur des listes, des fichiers ou des dossiers »[160]. Comparativement, la Convention 108 du Conseil de l'Europe relative au traitement d'informations était moins précise[161] que la définition de la CNIL. Il semble que l'Autorité Administrative Indépendante ait voulu garantir son champ de compétence en ne permettant pas au responsable du traitement de se soustraire à la loi «Informatique et Libertés» en lui laissant la possibilité de ne pas automatiser les fichiers. La directive 95/46/CE reprend la définition de la CNIL dans son article 3 et dispose que le texte s'applique « *au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personne contenues ou appelées à figurer dans un fichier ».*

62. La notion de fichier est définie à l'article 2, c) de la directive 95/46/CE « comme tout ensemble structuré de données à caractère personnel accessible selon des critères déterminé, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ». Le 27ième considérant de la directive relatif à la mise en œuvre manuelle du traitement précise que le texte ne s'applique pas aux dossiers non structurés et laisse à la discrétion des Etats membres de l'Union Européenne le soin de définir les critères permettant de qualifier les notions d'ensemble structuré de données ainsi que les éléments permettant l'accès à cet ensemble.

63. Lors de la transposition, le législateur français a repris les définitions contenues dans la directive européenne. Cependant, la loi du 6 août 2004 ne fait pas référence à « *la structure centralisée ou décentralisée »* ni *« à la répartition fonctionnelle ou géographique ».* Il convient de remarquer également que le texte[162] antérieur à la loi de 2004 fait seulement référence aux fichiers sans en donner une définition, alors que la transposition de la directive fait référence aux « *traitements contenus dans un fichier ».* De

[160] CNIL, « *Dix ans d'Informatique et Libertés »,* Economica, 1988, p.36 ; et 8e rapport annuel, la doc. Fr. Coll rapports officiels, 1986, p.30.
[161] La Convention 108 du Conseil de l'Europe définissait le traitement d'informations par un « traitement n'impliquant pas nécessairement l'existence d'un fichier ».
[162] Loi informatique du 6 janvier 1978, ancienne.

fait, le champ d'application de la loi du 6 janvier 1978 est large[163] car il suffit que le traitement manuel réponde à une simple organisation pour que la loi «Informatique et Libertés» (LIL) trouve à s'appliquer. Il suffit d'un classement de tout document selon n'importe quel critère[164] pour que l'ensemble créé soit qualifié de fichier et soumis à l'ancienne loi de 1978, ou qualifié de traitement de données appelé à figurer dans un fichier comme en dispose l'article 2 de la loi du 6 août 2004[165]. Cependant, il n'apparait aucune précision en ce qui concerne les critères de forme ou de contenu permettant de qualifier les structurations mettant en place des fichiers ou des dossiers. Il convient donc de s'en remettre à l'interprétation de la jurisprudence et de la CNIL.

64. La Cour de Cassation indique, dans son arrêt du 3 novembre 1987, que la collecte d'informations sous la forme de dossier et non sous forme de traitement automatisé ne peut faire l'objet de poursuites sur le fondement de la loi «Informatique et Libertés» du 6 janvier 1978[166]. La CNIL n'a pas considéré cet arrêt comme étant un arrêt de principe dans son 8ième rapport annuel de 1987[167]. Il semble que le Conseil d'Etat ait également une conception stricte du traitement. En effet, par un arrêt du 26 novembre 2010, le Conseil ne considère pas qu'il y ait un traitement si un décret prévoit la tenue d'un dossier individuel des personnes en centre de rétention, même si les informations figurant dans un dossier constituent un « *ensemble structuré et stable de données accessibles selon des critères déterminés au sens de l'article 2 de la loi*[168] *»* du 6 janvier 1978 «Informatique et Libertés».

Les différentes interprétations dans le niveau de structuration des informations semblent démontrer qu'une réflexion sur le niveau de structuration pourrait être envisagée. Cependant, le nouveau Règlement Européen[169] concernant la réforme de la directive

---

[163] R.Perray, « Informatique, Introduction générale et champ d'application de la loi « Informatique et Libertés », J.Cl. Comm, fasc 274-10, mai 2016 ; DEBET, A. / MASSOT, J. / METALLINOS, N. « La protection des données à caractère personnel en droit français et européen », Informatique et Libertés coll. Les intégrales 2015, n°10, éd. Lextenso.

[164] A. Lucas, J.Devèze et J. Frayssinet, *Droit de l'informatique et de l'internet,* PUF. Thémis droit privé, 2001, §132. C'est-à-dire que l'organisation s'effectue grâce à des identifiants, un code, par ordre alphabétique ou chronologique.

[165] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004 page 14063.

[166] Cass. Crim., 3 novembre 1987, *Bull. Crim.* n° 382 ; *D.* 1988, p 17, note H. Maisl.

[167] La documentation française, coll, rapports officiels 1987.

[168] CE, 26 novembre 2006, n°323694, publié au recueil Lebon.

[169] Réforme de la protection des données: le Conseil adopte sa position en première lecture, Communiqué de presse 171/16 ; Justice

95/46/CE n'apporte pas plus de précisions en la matière et reprend les termes de la directive.

b) L'exclusion de la qualification de traitement dans le cas d'activités personnelles

65. L'exclusion des traitements dans le cadre d'activités exclusivement personnelles est une exception prévue par la directive européenne. Cette exception concerne les traitements statistiques réalisés par l'Institut National de la Statistique et des Etudes Economiques (INSEE) ou pour l'un des services statistiques ministériels[170], pour les traitements de données faisant l'objet d'une anonymisation à bref délai[171] ou les traitements justifiant d'intérêt public[172].

L'article 45 de la « LIL » du 6 janvier 1978 prévoyait, avant la réforme du 6 août 2004, que la loi ne s'applique qu'aux traitements manuels « *autres que ceux dont l'usage relevait du strict exercice du droit à la vie privée ».* La directive européenne et la loi «Informatique et Libertés» excluent du champ d'application de la protection les traitements pour l'exercice d'activités exclusivement personnelles ou domestiques.

66. La finalité de l'activité, critère insuffisant.- Il convient d'analyser la notion de traitement en rapport avec une activité exclusivement personnelle. Le 12ième considérant de la directive 95/46/CE dispose que « *doit être exclu le traitement de données effectué par une personne physique dans l'exercice (...) d'activités exclusivement personnelles ou domestiques, telles la correspondance et la tenue de répertoires d'adresses ».* Il semble, cependant, que la Cour de Justice de la Communauté Européenne (CJCE) ne fasse pas une application stricte de la directive : l'affaire *Bodil Lindqvist* du 6 novembre 2003 démontre que la directive laisse une marge d'interprétation à la Cour qui a estimé que l'activité d'un bénévole religieux qui publie des informations personnelles relatives aux personnes de la paroisse devait être interprétée *« comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes »*[173]. La décision de la CJCE semble tomber sous le sens compte tenu du caractère public et du critère du *« nombre indéfini de personnes »* que la Cour relève dans

[170] Article 8, I, 7 de la directive 95/46/CE.
[171] Article 8, II, directive op cit loci.
[172] Article 8, III, directive op cit loci.
[173] CJCE, 6 novembre 2003, affaire C-101/01, *Bodil Lindqvist, §47.*

sa décision. Plus récemment, la Cour de Justice de l'Union Européenne (CJUE) a affirmé que le dispositif de vidéosurveillance mis en place par un particulier afin d'assurer la sécurité de son domicile ne peut relever de l'exception visée à l'article 3, 2°) de la directive 95/46/CE, dès lors que l'utilisation du dispositif ne relève pas uniquement d'une utilisation personnelle ou domestique[174]. Il ressort de ces deux décisions de la Cour Européenne deux critères qu'il convient de mettre en lumière : le critère de l'accessibilité aux données et la nature de l'activité.

67. Le critère de l'accessibilité.- Dans l'arrêt *Bodil Linqvist* du 6 novembre 2003[175] la Cour de Justice de l'Union Européenne semble s'attacher au critère du nombre de personnes qui peuvent accéder aux informations collectées dans un agenda. De fait, il semble que l'exception prévue par la directive ne s'applique que par la combinaison des critères de l'activité exclusivement personnelle et d'un accès limité aux informations collectées[176]. Dans l'arrêt du 11 décembre 2014 *Riynes,* l'avocat général N. Jääskinen affirme dans ses conclusions que le seul critère de la limite d'accès à certaines personnes ne suffit pas à permettre l'application de l'exception prévue par l'article 3, 2°) de la directive. Il considère, en effet, que le caractère exclusivement personnel ou domestique est « *indispensable »*[177] . L'avocat général ajoute à cela que la finalité du traitement n'est pas de nature à déterminer l'objet de l'activité poursuivie[178].

Dans le cadre de l'utilisation des réseaux sociaux, l'avis du Groupe de travail de l'article 29 (G29) indique que l'exception visée par la directive peut s'appliquer dans le cadre d'une « *utilisation domestique ».* Mais le G29 ajoute une analyse objective disant que l'exception n'a pas lieu de s'appliquer lorsque l'utilisation en réseau a pour but le « *développement des associations, d'une entreprise »*, lorsque l'accès à la page est trop large, et sans limitation

[174] CJUE, 11 décembre 2014, affaire C-212/13, *Riynes,* §33. En l'espèce, la personne avait mis en place un dispositif de surveillance qui ne se contentait pas de filmer uniquement la porte d'entrée de son domicile, l'angle de prise de vue empiétait également sur la voie publique et cadrait également sur la porte voisine se trouvant en face.

[175] *op. cit. loci.*

[176] DEBET, A. / MASSOT, J. / METALLINOS, N. « La protection des données à caractère personnel en droit français et européen », Informatique et Libertés coll. Les intégrales 2015, n°10, éd. Lextenso.

[177] Voir les conclusions de l'avocat général Niilo Jääskinen, CJUE affaire *Riynes* (C121/13) du 10 juillet 2014, n°53 et 59, cf annexe n°1.

[178] Conclusions de l'avocat général Niilo Jääskinen, CJUE affaire *Riynes* (C121/13) du 10 juillet 2014, n° 47.

d'indexation sur un moteur de recherche[179]. Le G29 conclut que l'on ne peut en déduire qu'il s'agit d'une activité purement personnelle[180].

68. L'interprétation stricte de la CNIL.- La CNIL s'est également prononcée sur la notion de traitement de données personnelles à but exclusivement personnel, notamment en ce qui concerne l'utilisation de publications de blogs comme moyen de communication. En effet, dans sa délibération 2005-284, la CNIL dispense de formalités concernant l'utilisation de blog mais ajoute, néanmoins, que les éditeurs de blogs sont, de fait, soumis aux autres dispositions de la loi «Informatique et Libertés[181] ». La position de la CNIL est conforme à celle de la CJUE. Elle prend en compte le fait que les blogs sont accessibles à tout utilisateur d'Internet[182].

Dans le domaine des réseaux sociaux et des communications à caractère privé, la Cour de Cassation s'est prononcée et a écarté l'application de la LIL en indiquant que les réseaux « *n'étaient en l'espèce accessibles qu'aux seules personnes agréées par l'intéressé, en nombre très restreint »* celle-ci formant ainsi une « *communauté d'intérêt »*[183].

69. L'utilisation domestique et les dispositifs de surveillance.- Le critère de l'utilisation domestique pose, cependant, certaines questions compte tenu de l'émergence des nouvelles technologies de surveillance et d'identification des personnes qui ne sont pas soumises au champ d'application de la loi «Informatique et Libertés». Par exemple, il semble que certaines applications permettant l'enregistrement de l'empreinte digitale afin de sécuriser l'accès à son terminal mobile ou tablette ne soient pas soumises à l'application de la LIL. Il semble donc que *« la loi ne tire pas aujourd'hui toutes les conséquences de ces principes puisque si elle soumet à autorisation la collecte et le traitement des données biométriques, elle ne les conditionne nullement à une finalité particulière »* remarque le

---

[179] G29, Avis 5/2009 du groupe de travail de l'article 29, *WP 163,* relatif aux réseaux sociaux, adopté le 12 juin 2009.
[180] *Ibidem Avis du G29, n°46.*
[181] CNIL, délibération n°2005-285 du 22 novembre 2005, portant recommandation sur la mise en œuvre par des particuliers de sites web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle.
[182] CNIL, délibération n°2005-284 du 22 novembre 2005, dispensant de déclaration les sites web diffusants ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle.
[183] Cass. Civ. 1ière, 10 avril 2013, n°11-19530 publié au Bulletin, note. C. Moulin.

Sénateur MM. G. Gorce[184] au sujet du développement de l'utilisation du *Touch ID* distribué par l'entreprise américaine Apple. L'analyse de MM. G. Gorce doit être combinée avec l'apport de l'arrêt de la CJUE *Bidil Linqvist*[185] de 2003 concernant la mise en œuvre d'un dispositif de surveillance mis en place par un particulier dans un objectif d'utilisation à des fins domestiques. La Cour affirme que l'utilisation d'une caméra de surveillance à des fins domestiques doit se limiter uniquement à la surveillance des personnes qui se trouvent dans le cercle privé et restreint familial. Cependant, en matière de vidéosurveillance et de géolocalisation, il demeure que les informations collectées nécessitent l'intervention d'un prestataire technique qui agit dans un but professionnel et qui est, ainsi, soumis à l'application de la loi «Informatique et Libertés» car il est le responsable du traitement[186].

L'activité domestique n'exclut pas le but lucratif.- A l'origine, la proposition de règlement, dans son considérant 15, maintenait les critères de l'exception de l'activité exclusivement personnelle. La proposition excluait toute activité à but lucratif sur Internet. Elle précisait, cependant, que la dérogation s'appliquait aux carnets d'adresses et à l'échange de correspondances entre particuliers[187]. Cette disposition fut amendée car une activité domestique n'est pas exclue de toute forme de commerce. Ainsi, le Parlement Européen autorise les activités lucratives sous la forme de « vente privée » si les actes « *sont exclusivement personnels, familiaux ou domestiques et sans lien aucun avec une activité professionnelle ou commerciale »*[188]. Cette dérogation s'applique également pour les publications de données à caractère personnel, dès que les garanties assurant un accès limité à un nombre de personnes sont remplies.

70. Exclusion des fournisseurs de moyens de traitement.- Les fournisseurs de solutions de traitement tels que les fournisseurs de services aux particuliers dans un but

[184] Proposition de loi n°361, *Visant à l'usage des techniques biométriques*, présenté au Sénat le 12 février 2014 par MM. G. Gorce.
[185] *op. cit. loci.*
[186] G29, avis 13/2011 du groupe de travail de l'article G29, *WP 185,* relatif aux services de géolocalisation des dispositifs mobiles intelligents, adopté le 16 mai 2011.
[187] Proposition de règlement du Parlement et de la Commission Européen, considérant 15, du 14 janvier 2012.
[188] Résolution, considérant 15 amendé.

domestique ne bénéficient pas de la dérogation car ceux-ci agissent dans un but professionnel et acquièrent la qualité de sous-traitants[189].

c) L'exclusion des copies temporaires

71. Dérogation limitée au fonctionnement du service.- L'exclusion de l'application de la loi «Informatique et Libertés» est visée à l'article 4 qui dispose que les « *copies temporaires qui sont faites dans un cadre d'activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises »*[190].

72. Justification de la diminution du champ de protection.- Selon le rapport Türk 1, la diminution du champ de protection des données à caractère personnel se justifie lorsqu'il s'agit de « prendre en compte les spécificités d'internet et des réseaux numériques [191]». Cette exception vise notamment l'utilisation de serveurs *proxy* qui ont pour fonction d'augmenter les performances des réseaux « *en mémorisant temporairement les adresses des internautes et les sites web consultés afin qu'il ne soit pas nécessaire d'accéder au serveur initial (...) en cas de nouvelle requête [192]».* L'exclusion du champ d'application dans le cadre des copies temporaires se justifie également par la volonté d'optimisation des réseaux internet. Le caractère temporaire du stockage de ces informations n'entrainerait aucune remise en question des droits des personnes, comme le droit d'opposition, en raison du caractère temporaire de la collecte et du stockage des informations[193]. De plus, le stockage temporaire ne présenterait « *aucun danger pour les internautes, compte tenu de leur effacement rapide par les serveurs proxy[194] ».* Ainsi, la régulation et l'optimisation des réseaux internet serait un des critères légitimant une diminution du champ de protection des données à caractère personnel.

---

[189] Article 3, II, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[190] Article 4, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[191] Rapport Türk I. fait au nom de la commission des lois, déposé le 19 mars 2003 page 49.
[192] Rapport Gouzes, *relatif à la* protection des personnes physiques *à l'égard des* traitements de données à caractère personnel *et modifiant la loi n° 78-17 du 6 janvier 1978 relative à* l'informatique, aux fichiers et aux libertés, page 31.
[193] Rapport Türk, op.cit.loci.
[194] Rapport Gouzes, op. cit. loci.

73. Critères d'application stricte de la dérogation.- La dérogation ne pourra être appliquée que si les conditions de l'article 4 de la loi sont remplies. Il est impératif que les traitements concernés aient pour finalité « de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises[195] ». De plus, la dérogation ne s'applique qu'aux copies temporaires et dans le cadre d'activités techniques dont l'objectif est « la transmission et la fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données ».

Ces exigences se retrouvent également visées à l'article 13 de la directive 2000/31/CE relative au commerce électronique du 8 juin 2000[196], transposée en droit français par la Loi pour la Confiance en l'Economie Numérique (LCEN) à l'article L.32-3-4 du Code des Postes et Communications Electroniques (CPCE) qui permet d'écarter la responsabilité des fournisseurs permettant un accès à des serveurs *proxys*[197].

Obligations des prestataires bénéficiant de l'exonération.- L'article 4 de loi «Informatique et Libertés» combinée à l'article 32-3-4 du CPCE dispose que pour bénéficier de la dérogation, les hébergeurs ne doivent exercer aucune intervention lors du traitement. Ils ne doivent faire subir aucune modification au contenu. Cependant, on note que les obligations des prestataires peuvent être difficiles à mettre en œuvre car ceux-ci doivent mettre en place toutes les mesures afin d'éviter tout détournement de la finalité. Cette obligation nécessite une intervention des prestataires afin qu'ils puissent garantir la sécurité des informations traitées. De plus, l'exonération visée à l'article L. 32-3-4 du Code des Postes et Communications Electroniques est écartée lorsque le prestataire conserve les fichiers *cache* au-delà de la durée nécessaire de ce que prévoit le principe d'accessibilité du traitement[198]. Ce principe est prédéfini par la finalité du traitement.

---

[195] Article 4, LIL, *op. cit. loci.*

[196] Directive 2000/31/CE du Parlement Européen et du Conseil relative au commerce électronique dans le marché intérieur du 8 juin 2000.

[197]« Toute personne assurant, dans le seul but de rendre plus efficace leur transmission ultérieure, une activité de stockage automatique, intermédiaire et temporaire des contenus que dans les cas suivant : Voir sa responsabilité civile ou pénale engagée dans l'un des cas suivant :

1° Elle a modifié ces contenus, ne s'est pas conformée à leurs conditions d'accès et aux règles usuelles concernant leur mise à jour ou a entravé l'utilisation licite et usuelle de la technologie utilisée pour obtenir des données ;

2° Elle n'a pas agi avec promptitude pour retirer les contenus qu'elle a stockés ou pour en rendre l'accès impossible, dès qu'elle a effectivement eu connaissance, soit du fait que les contenus transmis initialement ont été retirés du réseau, soit du fait que l'accès aux contenus transmis initialement a été rendu impossible, soit du fait que les autorités judiciaires ont ordonné de retirer du réseau les contenus transmis initialement ou d'en rendre l'accès impossible ».

[198] Cass. Civ. 1ère, 12 juillet 2012, n°11-15165 et 11-15188, publié au bulletin.

De fait, comme le fait remarquer le Groupe de Travail de l'article 29, le prestataire perdrait sa qualité d'hébergeur et pourrait être tenu pour responsable de la diffusion des données personnelles contenues dans le cache. Le G29 qualifie cette opération de « réplication indépendante » et pourrait qualifier le prestataire de responsable du traitement au sens de l'article 2 de la loi «Informatique et Libertés[199] ».

74. Moteurs de recherche et cybersurveillance, responsables du traitement.- Le groupe de travail de « l'article 29 » affirme que les moteurs de recherche doivent être à même d'accéder aux demandes de rectification ou d'effacement de données contenues dans les caches dès lors « *que ces données ne correspondent plus au contenu publié sur Internet par le responsable du traitement »*[200]. Cette affirmation permet de considérer les moteurs de recherche comme responsables du traitement au sens de l'article 2 de la loi «Informatique et Libertés»[201].

La CNIL apporte une nuance quant à la qualification des moteurs de recherche de « responsables du traitement ». En effet, la Commission considère que les éditeurs de données ont l'obligation de s'assurer de l'effacement des caches auprès des moteurs de recherche, notamment lorsque la publication est illicite au sens de l'article 6, 1°) de la loi «Informatique et Libertés»[202].

Le traitement des fichiers *cache* concerne également les risques liés à la surveillance des salariés par l'employeur. En effet, l'utilisation des serveurs *proxy* au sein de l'entreprise permet à l'employeur de connaître l'activité des salariés notamment vis-à-vis de « l'utilisation d'internet »[203]. La fonction de mémorisation des serveurs *proxy* permet à l'employeur de connaître l'adresse IP de l'utilisateur et, ainsi, d'avoir connaissance du contenu des recherches effectuées par le salarié.

75. Il semble donc que l'activité ou l'accès au contenu d'une navigation relève du champ de la protection des données à caractère personnel. Cette analyse permet de comprendre que la qualification de *données à caractère personnel* ne recouvre pas seulement des informations relatives à une identité ou relevant de la vie privée.

---

[199] G29, avis 1/2008 du groupe de travail G29, WP 148, relatif aux moteurs de recherche, 4 avril 2008.
[200] *Ibid.* G29, WP 148. Page 16.
[201] Article 2 de la loi « Informatique et Libertés » modifiée.
[202] CNIL, Délibération n°01-057, 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence.
[203] Rapport Bouchet, *La Cybersurveillance des salariés,* 2001.

Il convient d'exposer ce que recouvre la notion de données à caractère personnel ainsi que les critères emportant la qualification de données à caractère personnel.

Section 2 : Définition des données à caractère personnel

76. La notion de donnée à caractère personnel permet de protéger un grand nombre d'informations relatives à la vie privée de la personne concernée par le traitement. La notion n'a cessé d'évoluer tant dans sa définition légale que dans son interprétation (a). Cette évolution se justifie par la volonté d'étendre le champ de la protection de la loi «Informatique et Libertés» aux différents types de données. L'extension du champ de protection permet notamment de faire face au développement des outils informatiques et du « *tout numérique* ». La diversité de données impose l'analyse des éléments qui emportent la qualification du caractère personnel des données (b). Cependant, il convient également d'analyser les éléments permettant d'exclure la qualification (c).

a) La notion de donnée à caractère personnel

77. Définition légale.- L'article 2, a) de la directive 95/46/CE reprend et complète la définition de la convention 108, en précisant qu'une donnée à caractère personnel est « *toute information concernant une personne physique identifiée ou identifiable (...) est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle et sociale* ». Cette définition est complétée par le considérant 26 de la directive qui dispose que « *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne.*[204] ». On remarque que la définition de la directive envisage tous les moyens de

[204] Directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, considérant n°26 page 3.

traitement mais également tous les types de données permettant d'identifier la personne concernée par le traitement.

78. Définition extensive par la loi n°78-17 de la « LIL ».– L'article 2, alinéa 2 de loi «Informatique et Libertés» reprend la directive 95/46/CE et intègre[205] en partie le considérant 26 précité : « *Constitue une donnée à caractère personnel toute information relative à une personne physique 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*[206] *».*

On s'aperçoit que plusieurs notions se dégagent des textes. En effet, certaines notions paraissent proches mais sont pourtant bien différentes.

79. Distinctions « *Information », « Donnée nominative »* et « *Donnée à caractère personnel ».-* A l' origine, l'article 4 de la loi «Informatique et Libertés» faisait référence aux « informations nominatives » en les définissant comme les « *informations qui permettent sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou une personne morale ».* Certains auteurs[207] considèrent que cette définition avait « le mérite » de prendre en considération les données anonymes, par opposition aux informations qui n'étaient pas « nominative[s] ». La convention 108 du 28 janvier 1981 du Conseil de l'Europe retiendra finalement la notion de « donnée à caractère personnel » car celle-ci est plus large. Les données à caractère personnel devant être considérées « *comme toute information concernant une personne physique identifiée ou identifiable*[208] *».*

---

[205] G**.** Desgens-Pasanau**,** « La protection des données personnelles », 2ème édition, Lextenso, 2012. P. 7 à 11.

[206] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 2 al 2.

[207] A. Debet, « *Le champ d'application matériel de la notion de traitement des données à caractère personnel »,* La protection des données à caractère personnel en droit Français et Européen, ed, Lextenso, 2015.

[208] Article 2 de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981.

Certains auteurs[209] remarquent que la notion d' « information nominative » ne se confond pas avec celle de « donnée nominative [210]» ni avec celle de « donnée à caractère personnel[211] ». En effet, il convient de distinguer l'*information* qui ne se confond pas avec la *donnée*. En d'autres termes, une donnée est une information qui est transformée, c'est-à-dire qu'elle est valorisée parce qu'elle a été l'objet d'un traitement et possède un ajout technologique qui rend son exploitation plus aisée[212].

De la même manière, le caractère *« nominatif »* ne se confond pas avec le caractère *« personnel ».* En effet, l'adjectif *nominatif* fait référence au nom et permet donc de confondre la personne physique concernée par le traitement alors que le caractère *personnel* renvoie à une personne déterminée mais n'a pas pour fonction de permettre l'indentification[213]. On conclut, en l'espèce, que la notion d'information nominative peut se rapporter à une personne déterminée mais ne permet pas de l'identifier. Il convient donc de se référer à la notion de finalité du traitement ; par exemple, si le traitement de ces informations à *caractère personnel* ne vise pas à identifier la personne, ce type de traitement n'entrerait pas dans le champ de protection des traitements permettant l'identification de la personne, ce qui peut « *induire une vision étroite menant souvent à une appréciation erronée »*[214]. Afin de permettre un champ d'application large de la loi, la CNIL a indiqué que la notion d'information nominative ne se confondait pas avec la notion de *donnée à caractère personnel*[215].

80. Une vision large par la CNIL de la notion d'information nominative.- C'est sur le fondement de l'article 1 de la Loi «Informatique et Libertés» que la CNIL interprète la notion d'identité comme se rapportant à de nombreux supports ou formes. C'est-à-dire qu'elle considère que ce qui permet de distinguer une personne d'une autre permet

---

[209] V.R Perray, *J-Cl. Communication,* Fascicule 4710, n°30 et s. 30 juillet 2014.
[210] Ibidem.
[211] Ibidem.
[212] C. Castets-Renard, « Droit de l'internet : droit français et européen », Coll. Monchrestien, Ed. Lextenso, p. 35. ; Voir aussi F. Lesaulnier, « *L'information nominative »,* thèse Paris II, 2005, page 17 in A. Debet, « *Le champ d'application matériel de la notion de traitement des données à caractère personnel »,* La protection des données à caractère personnel en droit Français et Européen, ed, Lextenso, 2015 ; Le Clainche**,** J. La protection des données personnelles nominatives dans le cadre de la recherche dans le domaine de la santé Université Montpellier I Faculté de droit, des Sciences Economiques et de Gestion, 2008.
[213] *Ibid* thèse précitée p.14 et s.
[214] A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet,* PUF, Coll. Thèmis Droit privé, 2001, n°1111.
[215] CNIL, délibération n°93-032 du 6 avril 1993, *in* 14ième rapport annuel, La Doc. Fr., coll. Rapports officiels, 1994, page 59.

l'identification de la personne. Ainsi, la Commission qualifie d'informations ou de données nominatives une photographie, une bande sonore ou une image fixe ou animée, une vidéo dès lors que les individus sont reconnaissables[216], des factures[217], un code barre[218] ainsi que les empreintes digitales[219]. Cette interprétation large de la notion d'*informations nominatives* se justifie par le risque de ré-identification de la personne par recoupements des données[220]. Cette interprétation large de la notion a été confortée par une décision du Conseil d'Etat du 7 juin 1995 qui a considéré que le traitement en matière de segmentation comportementale constituait un traitement automatisé et permettait, de fait, d'associer le traitement statistique à une personne identifiable[221]. La CNIL a confirmé son interprétation extensive à plusieurs reprises. Dans le même sens, la Commission considère que les photographies d'un immeuble constituent des données nominatives en ce sens « *qu'elles permettent de rattacher une photo d'immeuble à une personne physique »*[222].

81. L'abandon de la notion d'*Information Nominative* au profit de la notion de *donnée caractère personnel*.- La notion d'information nominative dans son interprétation large, risquait de ne pas tenir compte de la réelle utilisation de l'information car elle s'attache aux effets produits dans un contexte déterminé et ne prend pas en compte le réel potentiel de rattachement à une personne physique[223]. La CNIL retient donc la notion de « donnée à caractère personnel » qui permet de mieux tenir compte des nouvelles capacités technologiques à rendre une information significative. Comme le remarquent certains auteurs, l'emploi des termes « données à caractère personnel » permet de tenir compte des

---

[216] N. Mallet-Pujol, « *Collecte, Utilisation et Diffusion des Données Nominatives à des Fins d'Enseignements et de Recherche, »* 2002, page 7, http://edutice.archives-ouvertes.fr/edutice-00000033 ; P.Murat, « *le contrôle de l'image de la personne en droit civil », l'image, Dalloz, Coll. Travaux de l'association* Henri Capitant, 2005, page 21.

[217] CNIL, Délibération n°80-016 du 6 mai 1980 concernant les traitements automatisés d'informations nominatives relatives à la consommation de gaz, d'électricité.

[218] CNIL, Délibération n°98.041 du 28 avril 1998 portant recommandation sur l'utilisation des systèmes de vote par codes-barres dans le cadre d'élections par correspondance pour les élections professionnelles.

[219] CNIL, Voix, image et protection des données personnelles, La Doc. Fr., 1996, page 22.

[220] CNIL, délibération n°93-032 du 6 avril 1993 ; CNIL, 16ième rapport annuel, La Doc. Fr.coll. rapports officiels, 1996, page 31.

[221] CE, 7 juin 1995, n°148659, publié au recueil Lebon, *Caisse régionale du crédit agricole de Dordogne ; Juris-Data* °1995-043340, *AJDA* 1996, page 162, note J.Frayssinet.

[222] CNIL, 23ième *Rapport annuel,* La Doc. Fr., coll. Rapports officiels, 2002, page 143.

[223] CE, 7 octobre 1998, n°186073, publié au recueil Lebon ; CNIL, Délibération n°80-34 du 21 octobre 1980 ; Délibération n°95-144 du 7 novembre 1999.

informations permettant une identification indirecte[224], notamment en matière de profilage[225] qui n'implique pas systématiquement l'identification de la personne.

Le groupe de travail de l'article 29 adopte une conception extensive de la notion de donnée à caractère personnel en développant ainsi quatre points essentiels de la définition des données à caractère personnel, à savoir toute « *information*, *concernant une personne physique*, *identifiée ou identifiable*»[226]. Pour retenir le *caractère personnel,* le G29 se réfère à la finalité « ultime » des règles relatives à la protection des données à caractère personnel visée à l'article 1 de la directive 95/46/CE dont l'objet est de « *protéger les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, à l'égard du traitement des données à caractère personnel »*[227].

La jurisprudence européenne a suivi cette interprétation large dans l'affaire *Bodil Linqvist* et considère que cette interprétation s'applique indifféremment à toutes les activités professionnelles, aux coordonnées téléphoniques, aux passe-temps, à des données déjà rendues publiques, aux empreintes digitales et aux profils ADN.

82. Transposition en droit interne de 2004, la limitation du champ d'application de la loi.- Lors de la transposition de la directive en 2004, le législateur a disposé que pour permettre la qualification de donnée à caractère personnel il convenait de « *considérer l'ensemble des moyens en vue de permettre l'identification de la personne dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».* Cette disposition de la loi vise à introduire le cas de l'anonymisation[228] des données qui peuvent encore permettre l'identification de la personne concernée par le traitement, par la mise

---

[224] *Ibid.*

[225] « Le profilage est une technique de surveillance ou d'exploitation des données qui permet sur la base des profils établis différentes actions, mesures ou décisions touchant les personnes concernées dans le cadre de finalités diverses. La technique ne consiste pas, à la base, à surveiller un individu en particulier pour une raison déterminée, mais à repérer des individus qui pourraient être sujets d'une surveillance ou d'une attention particulière ». J.Ph. Walter, *Le profilage des individus à l'heure du cyberespace : un défi pour le respect du droit à la protection des données*, disponible sur :
http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD_documents/Profilage%20doc%20F.pdf

[226] Groupe de travail « article 29 » sur la protection des données, avis adopté le 20 juin 2007, WP136.

[227] *Ibid. page 4.*

[228] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

œuvre d' « *efforts exceptionnels »*[229]. Le texte final fait référence aux « *moyens en vue »* de permettre d'identifier une personne alors que le considérant 26 de la directive 95/46/CE visait les moyens « *susceptibles d'être raisonnablement mis en œuvre »*. La transposition en droit interne a donc un champ d'application plus large que la directive. Cela entraîne un affaiblissement du pouvoir du responsable du traitement qui ne pourra se prévaloir du caractère anonyme des données que dans certaines conditions[230].

La définition de *donnée à caractère personnel* permet de dégager une conception de ce que recouvre le *caractère personnel*. Elle permet également une analyse objective des différentes données, autorisant ainsi une interprétation reposant sur des critères objectifs tels que : la capacité d'une donnée à être identifiante et le risque élevé ou non d'atteinte à la vie privée. Elle permet également de classer les données selon leur forme (image, son, statistiques etc.).

b) Les critères permettant la qualification de donnée à caractère personnel

83. Le critère fonctionnel, la donnée identifiante.- Le contenu seul de l'information ne permet pas l'application ou l'exclusion de la protection de la loi «Informatique et Libertés», c'est pour cela qu'il convient de se tourner vers une analyse des *capacités* d'une donnée à identifier ou non une personne. Les données dont la fonction est de permettre l'identification directe de la personne est le premier critère permettant de dégager la *fonction* d'une donnée[231]. L'identification de la personne recouvre « *l'identité physique, physiologique, psychique, économique, culturelle ou sociale*[232] *».* La définition permet également d'inclure dans le champ de protection de la loi «Informatique et Libertés» les données qui rendent possible l'identification. L'article 2 de la directive 95/46/CE permet d'envisager les différents types d'identité en dressant une liste de données se rapportant à une personne[233]. Cependant, la loi «Informatique et Libertés» fait référence à une notion plus large de l'identité puisqu'elle renvoie aux « *éléments qui [lui] sont propres »* à une

---

[229] Ibidem.
[230] Ibidem.
[231] R.PERRAY, « *Informatique, Introduction générale et champ d'application de la loi « Informatique et Libertés »,* J.Cl. Comm, fasc 274-10, mai 2016.
[232] Convention n°108 du Conseil de l'Europe, 28 janvier 1981, article 2.
[233] L'article 2 de la directive 95/46/CE vise les éléments qui se rapportent à l'identité qui peut être physique, physiologique, psychique, économique, culturelle ou sociale.

personne, que ces éléments soient pris seuls ou dans un ensemble[234]. Le champ d'application large de la définition se justifie par les multiples significations d'une donnée. Par exemple, le poids d'une personne peut être une donnée objective lorsqu'elle est exprimée en kilogramme, mais elle devient subjective lorsque cette donnée permet d'en conclure une surcharge pondérale[235]. En d'autres termes, les éléments se rapportant à l'identité permettent de singulariser la personne concernée par le traitement, que les données soient « objectives ou subjectives [236]» et quel que soit « le support technique utilisé[237] ».

84. Le critère substantiel, le rattachement à une personne.- Tant pour la directive 95/46/CE que pour la loi «Informatique et Libertés», une donnée est qualifiée de personnelle dès lors qu'elle entretient un lien permettant de la *rattacher* à une personne[238]. Cette définition permet de faire entrer dans le champ de protection de la loi, les données qui ne permettent pas, à elles *seules,* d'identifier une personne physique ; c'est-à-dire que ces données constituent un faisceau d'informations permettant d'identifier une personne ou de la rendre identifiable[239]. La prise en considération de ces données permet d'intégrer les nouveaux types de technologies de traitement qui sont visés par le 16ième considérant de la directive 95/46/CE qui reconnaît « l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données ».

85. L'impact sur la personne, la position du G29.- Le groupe de travail indique qu'une donnée est dite *à caractère personnel* dès lors qu'elle peut être rattachée à la

---

[234] CJUE, Affaires jointes C141/12 et C-372/12, Y.S contre *Minister voor Immigratie en Asiel et Minister voor Immigratie, Intergratie en Asiel c. M. et S.* 17 juillet 2014.
[235] C'est ce que remarque l'avocat général E. Sharpston dans ses conclusions dans les affaires jointes précitées *note 104.*
[236] G29, WP 136, Avis 4/2007 relatif au concept de données à caractère personnel, adopté le 20 juin 2007, page 7.
[237] *Ibid.*
[238] A. Debet, « *Le champ d'application matériel de la notion de traitement des données à caractère personnel »,* La protection des données à caractère personnel en droit Français et Européen, ed, Lextenso, 2015.
[239] CNIL, 17ième rapport annuel, relatifs aux informations recueillies sur un forum de discussion sur internet, la doc. Fr. coll. Raports officiels, 1997, page 92 ; voir aussi, G**.** Desgens-Pasanau**,** « La protection des données personnelles », 2ème édition, Lextenso, 2012, p13 et s.

personne concernée par le traitement[240]. Le G29 précise qu'une donnée qui est susceptible d'avoir un « impact » sur la personne, quel que soit le moyen de traitement (informatique ou manuel) utilisé, entraine la qualification de donnée *à caractère personnel*[241]. De plus, le groupe de travail retient que les données à caractère personnel recouvrent, d'une part les informations « objectives » comme les « particularités sanguines de la personne concernée », et, d'autre part, les informations subjectives donnant lieu à un « avis ou appréciation »[242]. Le groupe de travail de l'article 29 a adopte un avis intéressant car il déduit que le critère de véracité des données n'a aucune incidence sur la qualification de ces dernières. En d'autres termes, le G29 considère que, dès lors qu'une donnée peut permettre l'identification de la personne, même si elle se rapporte à la mauvaise identité, elle doit permettre l'application de la protection[243]. Le G29 ajoute qu'il n'est pas nécessaire que les données soient stockées ou structurées dans une base de données pour retenir la qualification de « caractère personnel »[244].

La position du G29 est explicite et permet de retenir la qualification de donnée à caractère personnel, dès lors que celle-ci a un impact sur la personne, ceci en raison de l'impact qu'elle a sur la vie privée de la personne concernée et, à plus forte raison, si cette donnée présente une caractère confidentiel. On peut en déduire que lorsque la donnée ne présente pas les critères visés ci-dessus, elle permet d'exclure la qualification de donnée à caractère personnel.

c) L'exclusion de la qualification du caractère personnel

86. La neutralité des données.- Tout au long de notre étude, notre objectif est de démontrer qu'aucune donnée collectée ou traitée n'est anodine[245] ; c'est-à-dire qu'il convient de reprendre le raisonnement de la CNIL qui affirme qu'il ne faut pas sous-estimer le potentiel « indiscret[246] » des données « réputées non sensibles[247] ». Certains

[240] G29 avis 4/2007, WP136 op. cit .loci.
[241] G29, avis WP 105, relatifs aux questions de protection des données liées à la technologie RFID, 19 janvier 2009 page 9.
[242] Avis WP 136 *op. cit. loci.* ; CJUE, 17 juillet 2014, affaires jointes C-141/12 et C-372/12 *op. cit. loci.*
[243] Ibidem.
[244] Ibidem.
[245] C**.** Castet-Renard**,** « Droit de l'internet ; Droit français et européen », Montchrestien, éd. Lextenso, 2012. P. 6.
[246] Rapport Tricot de la CNIL, La. Doc. Fr. coll. Rapport officiels, 1975, page 47.

auteurs affirment que tous les types de données « peuvent acquérir le caractère personnel, quel que soit le sens, l'utilité, l'usage et le volume, le support, le mode de représentation[248]. Ils démontrent également qu'il n'existe pas de donnée « anodine » car le sens d'une donnée peut évoluer en fonction du contexte et des associations effectuées[249]. Il est important de noter qu'une information prise hors de son contexte peut faire l'objet d'une mauvaise interprétation, c'est-à-dire que la combinaison de cette donnée avec d'autres peut créer une information qui ne pouvait être permise si la donnée avait fait l'objet d'une analyse seule ; c'est ce que certains auteurs nomment l'effet *mosaïque*[250]. En effet, il est possible de faire émerger un profil, d'analyser des comportements réels ou prédictifs, ayant pour origine des données ou des traces apparemment *anodines* comme, par exemple, avec l'utilisation de mots clefs saisis dans un moteur de recherche[251]. Il importe peu que les données soient vraies ou qu'elles ne soient que prédictives ; cette interprétation large du caractère personnel est approuvée par le G29[252].

87. Les données ne portant pas atteinte au droit à la vie privée.- L'objectif de la loi «Informatique et Libertés» est de garantir le droit à la vie privée de la personne concernée par le traitement tel qu'il est visé par l'article 9 du Code Civil. Mais, au-delà d'assurer la garantie de l'exercice d'un droit fondamental, elle permet de protéger un ensemble de droits et libertés de la personne concernée par le traitement. En somme, le simple fait que les données ne se rapportent pas à des éléments de la vie privée ne permet pas d'écarter la protection des données à caractère personnel. Il convient de conclure que ces deux notions sont complémentaires ou qu'elles doivent, pour le moins, être combinées[253]. Les nouvelles formes[254] de collectes de traitement des données ne permettent

---

[247] Ibidem.
[248] A. Lucas, J. Devèze et J. Frayssinet, « *Droit de l'informatique et de l'internet »,* PUF, coll. Thèmis droit privé, 2001, n°113.
[249] « *Les sociétés de ventes par correspondance ne demandent pas l'âge, car cela est mal perçu ; mais grâce aux tables d'attribution des prénoms de l'INSEE, elles déduisent avec une forte probabilité l'âge des personnes » :* A. Lucas, J. Devèze et J. Frayssinet, *op. cit. loci.*
[250] O. Tene, J. Polonetsky, « *Big Data For All : Privacy And User Control In The Age Of Analytics »,* Northwestern Journal Of Technologie And Intellectual Property, Volume 11, ISS 5, Page 251.
[251] J-C. Cointot, Y. Eychenne, « La révolution Big Data, nos données au cœur de la transformation de l'entreprise », Ed. Dunod, 2014.
[252] G29, Avis 4/2007 op. cit. loci.
[253] CJCE Airey c. Irlande, série affaires n°41, §26, du 9 octobre 1979 ; 13 mai 1980, Artico c. Italie 13 mai 1980 ; CJCE, Productores de Mùsica de España c. Telefònica des España SAU, affaire C-275/06 du 29 janvier 2008.
[254] P. Delort, « Le Big Data », Coll. « *Que sais-je »,* Ed. Puf, 2015, p. 29.

pas de connaître à l'avance quels types de données seraient susceptibles de porter atteinte aux droits et libertés d'une personne. Il convient de retenir que « l'atteinte ne concerne pas que la vie privée, mais, tous les aspects de vie personnelle [255]». La protection des données personnelles recouvre, non seulement la notion de vie privée, mais, également, ce qui se rapporte largement à la vie personnelle, professionnelle, ou publique. En d'autres termes, même si les informations ne sont pas couvertes par le secret professionnel ou qu'elles ne revêtent pas un caractère confidentiel intrinsèque à la fonction de celui qui les détient, la protection relative aux données à caractère personnel s'applique.
L'application large de la notion de donnée à caractère personnel se justifie d'autant plus avec l'évolution des moyens de collecte et de traitement des données qui entraîne une grande diversité de données générées.

Conclusion.- La notion de traitement doit être considérée de façon large. Au-delà de l'aspect technique, il convient de retenir que lorsqu'un fichier contient une information concernant une personne, le traitement doit être analysé en considération du régime de protection prévu par l'article 2 de la loi n°78-17, du 6 janvier 1978. Enfin, la notion de *donnée à caractère personnel* doit également prendre en compte les informations qui se rapportent de façon directe ou indirecte à la personne, cette acception permettant d'envisager la diversité des données à caractère personnel.

Chapitre 2 : La diversité des données à caractère personnel

88. Les critères emportant la qualification de donnée à caractère personnel permettent de dresser la typologie des différentes données. La première distinction qui n'a pas fait l'objet d'une nouvelle définition légale, est la distinction permettant l'identification directe ou indirecte de la personne concernée (section 1). Cette distinction fait cependant l'objet d'une interprétation large et permet d'inclure des données issues des nouveaux traitements permettant la déduction d'informations sensibles (section 2).

[255] I. Coulibaly « La protection des données à caractère personnel dans le domaine de la recherche scientifique », Thèse de droit privée, 2011, p.86.

Section 1 : Les données permettant l'identification directe ou indirecte

Les données à caractère personnel font référence à une personne (a), mais, selon le contexte dans lequel elles sont traitées, les données peuvent se rapporter indirectement à une personne (b). De plus, l'évolution des TIC permet à l'utilisateur d'agir sous une nouvelle forme d'identité. Le Conseil d'Etat remarque[256] qu'il est aujourd'hui primordial de prendre en compte la dématérialisation de l'identité (c) afin de garantir une protection des données à caractère personnel pleine et entière.

a) L'identification immédiate

89. L'identification immédiate fait référence à l'identité civile, c'est-à-dire à ce qui permet de singulariser une personne grâce à son nom, prénom, sexe, date et lieu de naissance[257]. Il ressort que, pour retenir la qualification de donnée personnelle, les identifiants doivent se rapporter à la personne concernée. Ainsi, dans une affaire[258], il a été considéré que la mise en ligne d'un fichier composé exclusivement de patronymes par ville ne constituait pas un fichier risquant d'entraîner l'identification directe ou indirecte d'une personne. Il semble que le simple fait de faire figurer le nom dans un fichier ne suffise pas à entrainer l'application de la loi «Informatique et Libertés». Cependant, il conviendra également de démontrer que la finalité du traitement ne permet pas d'entrainer une identification[259]. Il faut donc que le nom soit associé à d'autres données pour que la loi «Informatique et Libertés» puisse s'appliquer.

90. Les données issues du « corps humain » -. Outre l'identité civile, l'identification d'une personne peut découler d'éléments issus du corps humain. Les particularités physiques peuvent également permettre d'identifier une personne. La CNIL indique que « pour un informaticien, une image numérisée ou une voix numérisée constituent des

---

[256] Conseil d'Etat, Rapport, « Le numérique et les droits fondamentaux », 2014.
[257] Décret n°2013-175 du 26 février 2013, portant création d'un traitement automatisé de données à caractère personnel dénommé « Nutrinet-Santé », JORF n°0050 du 28 février 2013 page 3323.
[258] TGI Paris, 22 septembre 2008, *Kalid O. contre Notrefamille.com,* Note E. Derieux, *Legipresse 2008,* n°257, §255-10, disponible sur www.legalis.net.
[259] *Ibidem*, La protection par la LIL ne trouve donc pas à s'appliquer lorsque « *le recensement, sans autre précisions, de plusieurs naissances de personnes au nom du demandeur dans un département, réparties dans deux communes, mais sans interdiction, mais sans indication, ni de la date précise de ces naissances, ni des prénoms ».*

données qu'il est possible de traiter en ordinateur à l'égal d'un fichier de caractères alphanumériques […] il n'est pas nécessaire pour identifier une personne d'associer formellement un visage et un nom [260]». La physionomie d'une personne est un des éléments qui permettent d'identifier une personne. Ces données sont dites anthropologiques[261] ; par exemple, le poids, la taille, les mensurations sont autant d'éléments qui permettent d'identifier une personne[262]. La voix a été considérée comme étant une donnée à caractère personnel[263]. Le considérant n°14 de la directive 95/46CE indique que « compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données ». Il en va de même pour les analyses génétiques[264] ADN.

91. L' « identité » biométrique.- La biométrie désigne les techniques et les technologies de reconnaissance physique et biologique des personnes. Elle permet l'identification directe d'une personne. Les données biométriques sont considérées par la CNIL comme des données relatives à l'identité « à la différence de toute autre donnée d'identité, et, à plus forte raison de toute autre donnée à caractère personnel, la donnée biométrique n'est pas attribuée par un tiers ou choisie par la personne : elle est produite par le corps lui-même et le désigne ou le représente, lui et nul autre, de façon immuable. Elle appartient donc à la personne qui l'a générée[265] ». La Commission considère comme donnée à caractère personnel, les traces d'empreintes digitales « relevée[s] à l'occasion d'une enquête en vue de facilité[r] la recherche et l'identification par les services de police judicaire, des auteurs de crimes ou de délits afin de les déférer devant les tribunaux », elle

[260] CNIL, délibération n°94-095 du 15 novembre 1994 relative à la proposition modifiée de la directive du Conseil de l'Union Européenne relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données.
[261] Science de l'homme. Etude des êtres humains dans une perspective biologique et sociale. On distingue l'anthropologie physique, qui étudie l'évolution et l'adaptation des humains en tant qu'êtres biologiques, de l'anthropologie sociale et culturelle, qui étudie la vie des hommes en société à travers leur langue, leurs coutumes, leurs pratiques, leurs croyances, leurs mythes, leurs institutions. Définition de l'Association Française des Anthropologues.
[262] *Ibid délibération de la CNIL n°94-095 du 15 novembre 1994.*
[263] La « signature vocale », CNIL, Voix, Image et protection des données personnelles, La Doc. Fr., 1996.
[264] CNIL, 12ième rapport annuel, La Doc. Fr. coll. Rapports officiels, 1992, page 92.
[265] CNIL, communication du 28 décembre 2007, relatif à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données.

inclue également celles relatives aux personnes non identifiées[266] ou les données ayant fait l'objet d'un codage[267].

b) L'identification indirectement nominative

92. Les données indirectes, l'identité d'attribution.- Les identifiants sont les premiers moyens qui permettent l'identification, de façon indirecte, d'une personne. Les identifiants sont des données qui sont attribuées de façon unique à une personne et qui permettent de la distinguer d'un ensemble. Il convient de distinguer deux degrés d'identifiants : le premier est l'identifiant que l'on peut qualifier de non équivoque, c'est-à-dire qu'il n'est pas déterminé par la personne lors de l'attribution. Le second peut être qualifié d'équivoque : c'est le cas de l'utilisation de pseudonymes.

93. L'identification via les matricules.- Il s'agit ici des identifiants qui sont attribués de façon unique et dont le caractère sensible[268] provient du fait qu'ils sont constitués à partir d'éléments issus de l'état civil de la personne. Par exemple : le numéro figurant sur la Carte Nationale d'Identité est composé pour l'essentiel du nom de famille, du sexe, de la date de naissance et de l'adresse du détenteur[269]. Un deuxième exemple est le Numéro d'Inscription au Répertoire (NIR) qui devait être utilisé pour la mise en place du projet Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus (SAFARI) en 1971 et qui a entrainé l'adoption de la loi «Informatique et Libertés»[270]. L'utilisation du NIR ou une partie « non signifiante » de l'immatriculation a fait l'objet de nombreux débats lors de la mise en place du Dossier Médical Personnalisé : les moyens

---

[266] CNIL, délibération n°87-102 du 14 octobre 1986, concernant un projet de décret relatif au fichier automatisé des empreintes digitales géré par le Ministère de l'intérieur.
[267] CNIL, délibération n°87-106, du 3 novembre 1987, portant avis sur la mise en place par l'Office Français de Protection des Réfugiées et Apatrides d'un traitement automatisé relatif à la dactyloscopie des demandeurs du statut de réfugié.
[268] G**.** Desgens-Pasanau**,** « La protection des données personnelles », 2ème édition, Lextenso, 2012. 66.
[269] La carte d'identité et ses numéros, disponible sur http://www.carte-identite.fr/numero ; Mallet-Poujol, N. « Quels *droits pour l'individu face au risque d'un Etat Big Brother ?* », Cahiers Français, « La place de l'Etat aujourd'hui », Documentation française n°379, mars-avril 2014, p. 64.
[270] Voir supra introduction p5.

d'identification du patient sont prévus à l'article L.1111-8-1[271] qui dispose qu' « un identifiant de santé des bénéficiaires de l'assurance maladie pris en charge par un professionnel de santé ou un établissement de santé ou dans le cadre d'un réseau de santé » est utilisé pour la coordination des soins dispensés et pour la « conservation, l'hébergement et la transmission » des données de santé. L'Identifiant National de Santé (INS) est la cléf qui permet d'accéder aux informations du patient et à ses traitements médicaux.

94. La mise en place de l'Identifiant National de Santé (INS).- L'INS a été l'objet de tous les enjeux, tant dans sa définition juridique que sur la finalité de son contenu. L'INS est une donnée à caractère personnel car elle renvoie à une personne qui peut être identifiée, directement ou indirectement grâce à sa référence, à un numéro d'identification ou à des éléments qui lui sont propres. En effet, le premier projet de création de numéro d'identifiant santé consistait à reprendre le numéro de sécurité sociale car la création à partir de « rien » d'un nouveau numéro suppose la création de nouveaux algorithmes, de tester leur fiabilité, d'envisager toutes les compatibilités entre différents systèmes etc. Sans oublier le coût qu'aurait représenté sa création dans une conjoncture économique qui appelle à la raison. C'est pourquoi les instigateurs des premiers dossiers patients informatisés, conjointement aux services de la sécurité sociale, avaient d'abord émis l'idée de créer un numéro unique à partir du Numéro d'Inscription au Répertoire (NIR)[272]. Ce numéro est un numéro unique comme le prévoit l'article L.1111-8 du Code la santé publique.

L'objectif de l'utilisation d'un numéro unique, en s'appuyant sur le Répertoire National d'Indentification des Personnes Physiques (RNIPP) et sur le NIR dont la gestion a été confiée à l'INSEE par le décret n° 46-1432 du 14 juin 1946, avait pour objet d'utiliser le numéro de sécurité sociale comme identifiant de chaque personne physique comme en

[271] Issu de la loi n° 2007-1786 du 19 décembre 2007 de financement de la sécurité sociale pour 2008.

[272] Op. Cit. Selon le Rapport de BRAS d'octobre 2013 « Le NIR est un identifiant équivalent à la chaîne « Nom-Prénoms-Sexe-Date et Lieu de naissance ». Il s'en distingue essentiellement par le fait qu'il est plus court et fixe, et que son emploi évite donc des erreurs et des corrections, surtout si les NIR utilisés ont été préalablement certifiés (c'est-à-dire si on a vérifié qu'ils sont bien conformes au NIR délivré initialement à la personne). Il peut demeurer des incertitudes sur l'orthographe, sur les noms de naissance ou d'usage, ou sur les dates de naissance mais il n'est pas difficile, avec des outils informatiques modernes, de rapprocher deux fichiers nominatifs et, avec un peu de temps, de lever la plupart des incertitudes. Comme le savent les utilisateurs de moteurs de recherche sur Internet, un index numérique commun n'est pas du tout nécessaire pour croiser des fichiers nominatifs ou pour effectuer une recherche dans une base de données (comme c'était le cas dans les premiers temps de l'informatique).

dispose l'article L.114-12-1[273] du Code de sécurité sociale modifié. L'utilisation de ce numéro permettait d'obtenir une identification sûre, sans « doublon »[274] ni risque d'homonymie. Ce numéro reste une composante fiable d'identification car il est basé sur des éléments d'état civil. Malgré l'opportunité tant économique que pratique, l'utilisation du numéro de sécurité sociale suscite une peur de « fichage général » symbole d'une tentative d'immixtion de l'Etat dans la sphère privée des individus. L'INS peut donc se rapprocher du processus de l'Internet Protocol[275] qui est, selon la CNIL, une donnée sensible. En effet, La CNIL précise, dans son communiqué du 2 août 2007, que les plaques d'immatriculation et le numéro de téléphone sont des informations à caractère personnel et affirme que « l'adresse IP attribuée à un internaute lors des ses communications constitue une donnée à caractère personnel ». Par ailleurs, le jugement du Tribunal de Grande Instance (TGI) de Paris, daté du 24 juin 2009[276], confirme que l'adresse IP est bien une information à caractère personnel.

Il ne fait, alors, aucun doute que l'Identifiant National de Santé doit être qualifié de donnée à caractère personnel. De plus, le Conseil Constitutionnel admet[277] que le mécanisme de collecte de données est indirectement identifiant, comme les adresses IP qui sont des données à caractère personnel.

95. La nature de l'INS, la position du Conseil d'Etat.- L'INS pose également une difficulté concernant sa définition et sa nature. En effet, avant la promulgation de la loi de modernisation de notre système de santé[278], dans sa décision du 2 juillet 2007, le Conseil d'Etat[279] ne considère pas le numéro de sécurité sociale comme étant une donnée sensible. Dans cette décision, le Conseil d'Etat s'est prononcé à propos du décret[280] du 22 décembre 2005 qui détermine les conditions dans lesquelles des agents chargés du contrôle des

[273] Le répertoire contient les données communes d'identification des individus, les informations relatives à leur affiliation aux différents régimes concernés, de leur rattachement à l'organisme qui leur sert les prestations ou avantages, à la nature de ces derniers, ainsi que l'adresse déclarée aux organismes pour les percevoir.
[274] Op. Cit. Rapport Bras sur la gouvernance des données de santé page 39 note n°55.
[275] L'IP ou *Internet Protocol* est le protocole de communication de réseau informatique. L'adresse IP est le numéro qui identifie grâce à ce protocole chaque ordinateur ou tout matériel connecté à l'internet ou réseau utilisant l'Internet Protocol.
[276] TGI Paris, 3ième Ch., 24 juin 2009, RDLI 2009/51, n°1686.
[277] Conseil constitutionnel, 10 juin 2009, n° 2009-580 DC, JO 13 juin.
[278] Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JORF n°022
[279]Conseil d'État, 1ère et 6ème sous-sections réunies, 02/07/2007, décision N° 290593
[280] Décret n° 2005-1624 du 22 décembre 2005 relatif au suivi de la recherche d'emploi.

conditions de recherche d'emploi ont accès aux renseignements détenus par les administrations sociales et fiscales, ainsi que les institutions gestionnaires du régime d'assurance chômage. Le Conseil d'Etat indique que ce traitement relève de l'article 27 de la loi du 6 janvier 1978 et nécessite un avis motivé de la CNIL ainsi qu'un décret pris en conseil d'Etat mais ne reconnaît pas de manière explicite que le numéro de sécurité sociale est une donnée sensible.

A la lecture de l'article 27 de la loi du 6 janvier 1978, on s'aperçoit que le numéro de sécurité sociale n'est pas considéré explicitement comme une donnée sensible. En revanche, il l'est de façon implicite car le traitement qui porte sur le N.I.R est autorisé par décret et porte « sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques. ».

96. Le groupe de travail de « l'article 29 »[281] analyse ce numéro d'identification comme étant une donnée sensible, compte tenu de sa finalité. Son analyse est faite en application de la directive 95/46/CE relative à la protection des données personnelles et réalisée par le groupe des CNIL européennes. Si l'on reprend en substance cette analyse, le groupe de travail indique que « toutes les autres données - par exemple les données administratives (numéro de sécurité sociale, date d'admission à l'hôpital, etc.) – contenues dans les documents médicaux relatifs au traitement d'un patient doivent êtres considérées comme sensibles : si elles n'étaient pas pertinentes dans le cadre du traitement du patient, elles n'auraient pas été, et n'auraient pas dû être, incluses dans le dossier médical. ». Les membres du groupe de travail sont, par conséquent, d'avis que toutes les données contenues dans les documents médicaux, les dossiers médicaux électroniques (DME) et les systèmes électroniques soient considérées comme des données à caractère personnel sensibles. Elles sont donc soumises, non seulement à toutes les règles générales sur la protection des données à caractère personnel énoncées dans la directive, mais aussi, aux règles spéciales en matière de protection des données relatives au traitement des informations sensibles visées à l'article 8 de la directive.

Il peut paraître regrettable que ce groupe n'ait pas de pouvoir contraignant car si l'on s'interroge sur le rôle de l'identifiant de santé, on constate qu'il entre dans la catégorie des données qui permettent d'identifier un individu. D'autant plus que ce numéro figure dans le dossier médical du patient. A la lecture des caractéristiques de l'INS, l'ASIP Santé

[281] Avis du G29, Op. cit. P. 60.

indique que ce numéro n'est ni public ni secret mais il permet une authentification car il est unique. Or, l'article 2 de la loi du 6 janvier 1978 dispose qu'une donnée est à caractère personnel dès lors qu'elle fait référence à un numéro d'identification ou à des éléments qui lui sont propres.

97. Cependant, la CNIL est allée à l'encontre de sa politique de sectorisation des données en autorisant l'utilisation du NIR entre les différents organismes en relation avec le secteur de la santé. En effet, dans sa délibération du 20 février 2007, la Commission indique que « même si des mesures de protection toutes particulières étaient prises en ce qui concerne les procédures d'accès et d'authentification, l'utilisation directe d'un numéro aussi répandu que le NIR[282] » cela risque de provoquer la rupture du lien de « confiance entre les professionnels de santé et les patients ». La Commission ajoute que l'utilisation du NIR peut susciter des questions relatives à la légitimité de l'utilisation cet identifiant. La CNIL continue en relevant que malgré « de nouvelles procédures de certification », la création d'un nouvel identifiant « entraînerait des coûts supplémentaires et des délais de mise en œuvre plus longs [283]». La commission conclut en indiquant que « la création d'un identifiant de santé spécifique, généré à partir du Numéro d'Identification Inter-régime, certifié selon les procédures déjà éprouvées » serait une solution. Ce numéro « non signifiant, constituerait l'identifiant de santé utilisable dans l'ensemble du système de soins[284] ».

La Commission émet donc un avis qui transige entre la réutilisation en partie du NIR et la création d'un nouvel identifiant. Cette option permettrait de respecter la politique de cloisonnement des données en fonction de chaque secteur, tout en évitant une étape de plus dans la création d'une base de données nouvelle ; ceci améliorerait la sécurisation des données et limiterait les erreurs en cas d'homonymie.

Dans son rapport d'activité de 2013, la CNIL précise qu'elle n'a toujours pas été saisie « du projet de décret simple prévu par l'article L.1111-8-1 du Code de la santé publique qui doit fixer le choix de cet identifiant, ainsi que ses modalités d'utilisation. ».

---

[282] Délibération n° 2007-036 du 20 février 2007 portant avis sur deux projets d'arrêtés relatifs, d'une part, aux spécifications physiques et logiques de la carte d'assurance maladie et aux données y étant contenues et, d'autre part, aux conditions d'émission et de gestion des cartes d'assurance maladie.

[283] *Ibidem*.

[284] *Ibidem*.

Elle profite de la publication de son rapport d'activité[285] pour réaffirmer sa position par rapport à la création d'un numéro d'identification dans le secteur de la santé, en précisant qu'elle ne serait pas hostile à une évolution de sa part « à condition que l'utilisation du NIR dans la sphère de la santé aille de pair avec l'élévation de solides remparts vis-à-vis d'autres secteurs »[286]. Pour mettre en relation toutes les personnes inscrites au RNIPP et leur caisse d'affiliation au régime général, un répertoire a été créé en 1996 : le Répertoire National Inter-régime des bénéficiaires de l'Assurance Maladie (RNIAM). Ce répertoire est mis à jour par l'INSEE et c'est par son biais que les caisses d'assurance maladie ont accès aux données pour émettre la Carte Vitale.

La CNIL a, finalement, rendu un avis favorable à la création et à l'utilisation de l'INS dans sa délibération du 12 mai 2016, reprenant les conditions de sécurité et d'utilisation des référentiels de sécurité[287].

98. Suivant les recommandations de la CNIL, l'ASIP Santé a donc travaillé à l'élaboration d'un identifiant généré depuis le NIR car ce numéro pourrait permettre, à terme, de lancer le déploiement des DMP car il pourrait servir à l'ouverture du dossier et à sa tenue comme en dispose l'article L.161-36-1 du Code de la sécurité sociale. Ce numéro servirait également à la tenue du dossier pharmaceutique visé à l'article L.161-36-4-2 CSS. L'ASIP Santé travaille sur sa conception en collaboration avec les industriels et les acteurs de santé. Pour cela, elle a publié en novembre 2009[288] un dossier expliquant comment était conçu l'identifiant de santé, et un an plus tard, elle a indiqué que les développeurs ayant intégré l'algorithme dans leur logiciel permettant de générer l'identifiant national de santé pouvaient se faire référencer[289]. L'ASIP Santé a publié la version 1.1 du dossier de conception de l'identifiant de santé, le 5 mars 2014. Elle a également mis en place une méthode[290] de calcul permettant de générer un identifiant provisoire que l'agence nomme

---

[285] Rapport d'activité CNIL 2013, disponible sur *www.cnil.fr/documentation/rapports-dactivite.*
[286] Voir Rapport annuel CNIL 2013, page 10 disponible sur : http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_34e_Rapport_annuel_2013.pdf.
[287] CNIL, délibération n°2016-147 du 12 mai 2016, portant avis sur le projet de décret en Conseil d'Etat relatif au DMP.
[288] Concertation consultable sur http://esanté.gouv.fr.
[289] Communique de Presse du 9 juin 2010 Une première étape pour un identifiant national adapté à l'échange et au partage de données de santé disponible sur http://esante.gouv.fr/sites/default/files/CP_INS_ConventionASIP_CNDA_090610.pdf.
[290] Voir dossier de conception d'un INS-C annexe n°4.

« INS de Calcul » (INS-C). Déjà, en 2009, la CNIL indiquait que le texte devrait lui être soumis, or, dans son 34ème rapport d'activité, pour l'année 2013, la Commission déplorait implicitement ne pas avoir été consultée sur le projet de mise en place de l'INS-C[291]. Notons que le dossier pharmaceutique (DP) a mis en place un identifiant provisoire dans l'attente d'un identifiant définitif ; ceci risque d'être source de complexité lorsqu'il sera temps de joindre les numéros DP et les DMP car les identifiants de DP sont créés par des logiciels de gestion des officines et hébergés chez l'hébergeur agréé du DP.

La loi n°2007-127 du 30 janvier 2007 relative à l'organisation de certaines professions de santé a créé l'article L.1111-8-1 du Code de la santé publique remplaçant l'article 5 de la loi du 13 août 2004[292] et dispose qu' « un identifiant de santé des bénéficiaires de l'assurance maladie pris en charge par un professionnel de santé ou un établissement de santé ou dans le cadre d'un réseau de santé défini à l'article L.6321-1 est utilisé », dans un but de « coordination et de qualité des soins, pour la conservation, l'hébergement et la transmission des informations de santé ». Ce numéro est également utilisé pour l'ouverture et la gestion du DMP et du dossier pharmaceutique institué par l'article L.161-36-4-2 du même Code. L'article L.1111-8-1 ajoute qu'un décret « pris après avis de la Commission Nationale de l'Informatique et des Libertés, fixe le choix de cet identifiant ainsi que ses modalités d'utilisation ».

En résumé, selon l'ASIP Santé, après consultation de la CNIL, l'identifiant national de santé devra être unique : à chaque personne sera attribué un seul INS qu'elle gardera tout au long de sa vie.

Toujours selon l'ASIP-Santé, cet identifiant est « non signifiant » et sa divulgation ne devra pas permettre la « déduction d'informations sur la personne ». Il est certifié « sans doublon ». Enfin, l'identifiant doit être « non prédictible : la connaissance du NIR ou des traits d'identité de la personne n'autorisent pas la déduction de l'INS ». De même, « la connaissance de l'INS ne doit pas permettre de remonter au NIR de la personne. ». Concrètement, l'INS permet aux professionnels de santé de retrouver le dossier de santé du patient, qu'il s'agisse du dossier médical personnel, du dossier pharmaceutique ou d'autres dossiers médicaux. Associé à une procédure d'authentification, l'INS garantit la sécurité de l'accès au dossier informatisé du patient.

---

[291] Op. cit. note 1 page 51.

[292] Cet article disposait qu'un identifiant de santé devait être attribué à toutes les personnes prises en charge par un professionnel ou établissement de santé dans le cadre d'un réseau de santé même si cette dernière ne bénéficiait pas de l'assurance maladie.

Ces informations sont primordiales pour le professionnel de santé dans l'exercice de sa profession. Cependant, elles présentent également un enjeu important pour les hébergeurs de données de santé[293] qui commercialisent des logiciels de gestion à destination des professionnels de santé car ces protocoles doivent être respectés par les industriels afin qu'ils puissent obtenir l'agrément d'hébergeur de données de santé. C'est ici que l'enjeu commercial se joue pour les industriels.

99. Les données visant à porter une appréciation.- Selon la CNIL, toute donnée susceptible de dresser un profil vis-à-vis d'une personne est qualifiée de donnée à caractère personnel[294] au sens de l'article 4 de loi du 6 janvier 1978, dès lors que ces données révèlent des caractéristiques propres à la personne.

En matière bancaire, la Commission considère que les scores attribués à un client sont une donnée à caractère personnel car ils sont le résultat d'une analyse statistique révélant le niveau de risque présenté par l'emprunteur[295]. Cette information est non seulement une donnée à caractère personnel, mais elle permet aussi à la banque de prendre une décision quant la capacité de paiement de l'emprunteur.

c) La dématérialisation de l'identité

100. Les nouvelles formes d'identités.- La difficulté principale réside dans le fait que, sur internet, l'identité peut se présenter sous diverses formes. En effet, l'identité numérique ne se rapporte pas à l'identité civile décrite précédemment. Le plus souvent, l'utilisateur utilise une identité sous la forme de pseudonymes, de codes ou d'avatars[296] qui

---

[293] Cf infra, Chapitre 3, « le régime spécifique de la protection des données de santé à caractère personnel », p. 151.

[294] CNIL, Délibération n°02-017 du 21 mars 2002, portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opération de recrutement.

[295] CNIL, Délibération n°2008-198 du 9 juillet 2008 modifiant l'autorisation unique AU-005 relative à certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit.

[296] Rev. Correspondant Informatique et Libertés, *Identité numérique : quelle stratégie pour l'Etat ?, «* La question des identités numériques s'intéresse aux relations croisées entre un être humain, les avatars qui le représentent dans la sphère numérique et le sujet de droit qui le représente dans la sphère juridique.[…] En réponse, les géants de l'Internet, tels Google ou Facebook, qui disposent

sont des identités générées et déclarées par l'utilisateur lui-même. C'est l'identité numérique[297]. Aucune définition légale n'existe à ce jour, même dans la nouvelle loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité. On peut déduire que la notion de donnée à caractère personnel recouvre la notion d'identité numérique. L'article 226-4-1 du Code pénal est le seul texte qui vise directement le terme d'identité et qui permette d'en tirer les éléments constitutifs : « Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende[298] ». L'identité numérique se distingue par le fait qu'elle est polymorphe en ce sens où elle permet l'identification d'une personne, et, cette dernière est reconnue de façon certaine auprès de tiers avec un certain niveau de confiance. Par exemple : l'utilisation du dispositif associant un identifiant et un mot de passe, permet à l'utilisateur de se connecter grâce à ces identifiants à de nombreux sites tiers. L'utilisation du dispositif « Facebook Connect » permet à l'utilisateur de se connecter à des sites *via* son identité numérique crée sur Facebook. La notion d'identité numérique est une notion dont il est difficile de définir les contours, c'est l'enjeu qui est au cœur de la réflexion concernant l'application de la loi «Informatique et Libertés»[299].

101. L'adresse IP.- De nombreuses informations sont attribuées aux utilisateurs par des tiers opérateurs comme les Fournisseurs d'Accès Internet (FAI) ou les opérateurs de télécommunication : les coordonnées physiques permettant de localiser une personne, les logs, les certificats numériques ou l'adresse Internet Protocol (IP). L'attribution de

---

d'une part de marché considérable, investissent la question des identités numériques. D'ores et déjà aujourd'hui, beaucoup de services en ligne s'appuient sur l' « identité Google » ou l'« identité Facebook » de leurs clients, qui, au lieu de créer un compte, utilisent leur compte Google ou Facebook pour accéder au service. Il est très vraisemblable que cette tendance s'amplifie, ce qui pose de nombreuses questions (dépendance de « l'identité » des internautes à un positionnement commercial et à des conditions d'utilisation du service d'une société privée, utilisation de données personnelles par des sociétés dépendant de législations hors Union Européenne, maîtrise du niveau de confiance etc.). » Publié le 12 novembre 2013, CNRS, CIL.

[297] Il convient de préciser que le terme numérique recouvre une notion d'identification propre à une personne, l'identité numérisée, quant à elle, recouvre, la technique de dématérialisation des informations concernant la personne.

[298] Article 226-4-1 du Code Pénal, Loi n°2011-267 du 14 mars 2011 - art. 2.

[299] La CNIL qualifie ces nouveaux enjeux de « vaste chantier » : *Vie privée à l'horizon 2020,* Cahiers IP n°, 2012, page 38.

l'adresse IP est parfois un moyen plus sûr[300] d'identification que la référence à l'identité classique[301]. La qualification de l'adresse IP a donné lieu à un débat afin de savoir si elle était ou non une donnée à caractère personnel.

La CNIL s'est toujours prononcée de façon tranchée en affirmant que l'adresse IP est une donnée à caractère personnel. Le principal argument de la Commission étant que, si l'adresse IP n'est pas qualifiée de donnée à caractère personnel, c'est un secteur entier de l'économie numérique qui échappe à la protection garantie par la loi «Informatique et Libertés»[302].

102. La spécificité de l'adresse IP.- La particularité de l'adresse IP est qu'il s'agit d'une donnée qui est collectée de façon systématique et qu'il est possible de l'associer à un utilisateur et une date. Ce recoupement de données est possible par les FAI qui leur permettent de les relier à un compte utilisateur. Le plus généralement, l'adresse IP est statique[303], cela permet de connaître la localisation de l'utilisateur. La localisation géographique permet de distinguer l'utilisateur de tous les autres. Cette localisation devient donc *identifiante* car elle permet le traçage de la personne.

103. La position de la CNIL et du G29.- Les deux autorités sont d'accord pour considérer l'adresse IP comme une donnée qui permet d'identifier de façon directe ou indirecte la personne. Toutes deux affirment que l'adresse IP permet aux FAI d'identifier la personne, mais elles affirment aussi que cette identification est possible par les autres sites. En effet, chaque site consulté par l'utilisateur collecte les adresses IP mais, également, les traces de navigation ; lesquelles peuvent être associées pour permettre de réaliser une analyse du comportement[304]. L'adresse IP peut aussi prendre une valeur

[300] C'est une identification qui ne passe plus par la personne physique mais par son ordinateur, CNIL, *Votre ordinateur,* publication du 4 janvier 2016
[301] CNIL, 17ième rapport annuel, La Doc. Fr., Coll. Rapports officiels, 1997, p66.
[302] CNIL, 36ième rapport annuel d'activité 2015, « *Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles »,* Publié le 8 avril 2016 ; P-J Hustinx « La protection des données à caractère personne en ligne : la question de l'adresse IP », *Legicom*, 2009, n°42.
[303] Par opposition à une adresse IP dynamique qui permet de créer une adresse IP *éphémère* et qui est renouvelée à chaque connexion.
[304] G29, WP 136, Avis 4/2007, du 20 juin 2007 op. cit. loci.

unique identifiante dans le cadre de compilations de données collectées permettant ainsi de dresser le profil de la personne[305].

104. La nature de l'adresse IP.- Dès l'origine, le Conseil d'Etat ne remettait pas en cause le caractère personnel de l'adresse IP[306] mais cette position n'a pas toujours été suivie[307]. Le Conseil Constitutionnel a finalement mis un terme à la question qui était de savoir si l'adresse IP était une donnée à caractère personnel. En effet, lors de l'examen de la loi *HADOPI 2,* le Conseil Constitutionnel a admis que l'adresse IP était une donnée « permettant directement ou indirectement d'identifier les titulaires de l'accès à des services de communication au public en ligne » permettant « la mise en œuvre, par ces personnes privées, d'un traitement de données à caractère personnel relatives à des infractions [308]».

Enfin, la CJUE a estimé que « les adresses IP sont des données protégées à caractère personnel, car elles permettent l'identification précise des utilisateurs [309]». Le Conseil d'Etat a considéré, dans un arrêt du 12 mars 2014, que les adresses IP « associées aux contenus, date et heure des requêtes effectuées [310]» sont des données à caractère personnel. Il semble donc reconnu que l'adresse IP est une donnée à caractère personnel permettant l'identification directe ou indirecte d'une personne.

105. Le risque de ré-identification, les données anonymisées.- Une fois définis les critères permettant de retenir la qualification de donnée à caractère personnel, il convient d'analyser les critères permettant d'exclure la qualification en raison d'un niveau de sécurité suffisant ou les critères dus à une anonymisation qui ne permettrait pas le recoupement d'informations entrainant une identification indirecte ou par « faisceau ».

---

[305] C'est aussi le cas avec l'utilisation des cookies permettant l'optimisation de services lors de la consultation de sites ; CNIL, Délibération n°2013-420, du 3 janvier 2014, prononçant une sanction pécuniaire à la société *Google.*
[306] CE, 23 mai 2007, n°288149, inédit, SACEM et Autres.
[307] CA, Lyon, 17 Mars 2009, n°08/03020.
[308] Conseil Constitutionnel, 10 juin 2009, décision n°2009-580 DC, Loi favorisant la diffusion et la protection de la création sur internet, considérant n°7 ; C. Simon, « les adresses IP sont des données personnelles selon le Conseil Constitutionnel », *RLDI* 2009, n°59, page 114-115.
[309] CJUE, 24 novembre 2011, affaire C70-10, Scarlet Extended SA contre Société belge des auteurs, compositeurs et éditeurs SCRL ; Comm. Com. Electronique 2012, note A. Debet ; CJUE, 29 janvier 2008, affaire C-275/06, Promusicae contre Telefonica de Espana.
[310] CE, 12 mars 2014, n°353193, recueil Lebon.

La notion d'anonymat apparaît dans la directive 95/46/CE article 2, a) et le considérant n°26 qui indique que « pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne; que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable; que les codes de conduite au sens de l'article 27[311] peuvent être un instrument utile pour fournir des indications sur les moyens par lesquels les données peuvent être rendues anonymes et conservées sous une forme ne permettant plus l'identification de la personne concernée ».
L'article 2 de la loi «Informatique et Libertés» reprend, pour partie, le considérant 26 de la directive. Cependant, le législateur français a supprimé le terme « raisonnablement », ce qui entraîne une protection plus stricte de la loi «Informatique et Libertés» en matière de données personnelles, laissant au juge la liberté d'apprécier s'il s'agit d'une donnée anonyme ou à caractère personnel[312]. Il suffit donc qu'il soit possible de ré-identifier une personne ou qu'il existe une simple probabilité[313] pour que la qualification de donnée à caractère personnel s'applique. Certains auteurs considèrent que la « LIL » enlève « toute notion de proportionnalité dans la possibilité de ré-identification » et que la position du législateur s'écarte de la solution retenue par les autres Etats membres[314]. Néanmoins, si le législateur français avait conservé les termes faisant référence aux moyens susceptibles d'être « raisonnablement mis en œuvre » pour identifier une personne, cela n'aurait pas été de nature à permettre de contourner les difficultés de qualification que requièrent des moyens raisonnables permettant une ré-identification. En effet, cela nécessiterait, tout d'abord, que le responsable du traitement puisse connaître, à l'avance, les moyens présents

[311] Considérant 27, directive européenne 95/46/CE « Considérant que la protection des personnes doit s'appliquer aussi bien au traitement de données automatisé qu'au traitement manuel; que le champ de cette protection ne doit pas, en effet, dépendre des techniques utilisées, sauf à créer de graves risques de détournement; que, toutefois, s'agissant du traitement manuel, la présente directive ne couvre que les fichiers et ne s'applique pas aux dossiers non structurés; que, en particulier, le contenu d'un fichier doit être structuré selon des critères déterminés relatifs aux personnes permettant un accès facile aux données à caractère personnel; que, conformément à la définition figurant à l'article 2 point c), les différents critères permettant de déterminer les éléments d'un ensemble structuré de données à caractère personnel et les différents critères régissant l'accès à cet ensemble de données peuvent être définis par chaque État membre; que les dossiers ou ensembles de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application de la présente directive. »
[312] Données personnelles et société de l'information : rapport au Premier ministre sur la transposition en droit français de la directive numéro 95-46, 3 mars 1998, La Doc. Fr. coll. Rapports publics.
[313] G29, WP 37, du 21 novembre 2000 relatif au respect de la vie privée sur internet, §21.
[314] A.Debet, le champ d'application matériel de la loi Informatique et Libertés op.cit.loci.

et futurs dont dispose une personne ; ensuite, parce que les techniques de forage[315] de données combinées à de nombreuses bases de données multiplient les liens entre des données anonymes et des personnes[316]. Des moyens raisonnablement mis en œuvre ont fait l'objet d'une illustration en 2000 ; une étude universitaire a permis de démontrer qu'il était possible de ré-identifier 87% de la population nord américaine en combinant trois types de données anonymes : le code postal, le genre et la date de naissance[317].

106. L'extension de la qualification du caractère personnel.- Le G29, dans le cadre de la réforme du cadre Européen de protection des données personnelles, affirme que, même lorsqu'une donnée a fait l'objet d'une anonymisation, la qualification de donnée à caractère personnel doit trouver à s'appliquer[318]. Le G29 tire la conséquence de l'analyse du considérant 26 de la directive en affirmant, dans son avis concernant les données ouvertes, que dans la mesure où les données sont publiées à des fins de réutilisation, le terme « raisonnablement » ne peut pas s'appliquer car il est difficile de connaître les moyens que les tiers pourront mettre en œuvre pour tenter de ré-identifier des personnes au travers de données anonymisées.

La distinction entre les données à caractère personnel et les données anonymes est un enjeu primordial, en raison du développement des techniques et des capacités de ré-identification. Cet enjeu peut être illustré par l'augmentation du nombre de traces laissées sur internet par l'utilisateur, mais, également ,par l'augmentation du nombre d'objets connectés générant un grand nombre de données. La multiplication des données générées s'accompagne d'une augmentation des sources, augmentant de fait les capacités de recoupement des données, rendant le processus d'anonymisation incertain.

---

[315] Le forage de données peut être défini comme « l'application des techniques statistiques, d'analyse de données et d'intelligence artificielle à l'exploration et à l'analyse sans a priori de (souvent grandes) bases de données informatiques, en vue d'extraire des informations nouvelles et utiles pour le détenteur de ces données », S. Tuffery, Data mining et statistique décisionnelle, l'intelligence dans les bases de données, 2005, VII.

[316] G29, WP 136, Avis 4/2007 relatif au concept de données à caractère personnel, adopté le 20 juin 2007.

[317] Ibidem

[318] G29, Avis 06/2013, WP 207, adopté le 5 juin 2013, page 13.

Section 2 : Les données permettant la déduction d'informations sensibles

Il convient d'analyser ce que recouvre la notion de donnée sensible, notamment celles relatives à la santé de la personne (a) car le traitement de ces dernières sont susceptibles de créer un risque d'exclusion sociale (b).

a) Les données de santé à caractère personnel

L'étendue du domaine des données relatives à la santé est tel que nous pouvons la qualifier de « protéiforme », comme le suggère l'avocat et Consultant Informatique et Libertés (CIL) P. Desmarais. Cette nature « protéiforme » tient tant à la définition qu'aux finalités du traitement des données de santé.

107. Une définition protéiforme en raison de la multiplicité de ses sources.- Il n'existe pas de définition légale de la notion de donnée de santé. Il convient de définir les données de santé à travers ce qui les constitue. La directive européenne 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 indique, dans son considérant 33, que les données de santé sont susceptibles, du fait de leur nature, de porter atteinte aux libertés fondamentales ou à la vie privée. L'article 8 alinéa 1 de la même directive considère les données « relatives à la santé » comme des données « particulières ». La Commission Européenne estime donc que les données de santé relèvent des données à caractère personnel. En droit interne, les données de santé ne font pas, non plus, l'objet d'une définition légale. Cependant, les données à caractère personnel sont définies par la loi dite «Informatique et Libertés» du 6 janvier 1978 qui dispose dans son article 2 que : « Constitue une donnée à caractère personnel 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 ».

Depuis 2004[319], l'article 8 de la même loi dispose que les données qui font « apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques,

[319] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci » constituent une information à caractère personnel. Cette dernière disposition place donc les données de santé dans la catégorie des informations à caractère personnel. Le Code de la santé publique emploie d'ailleurs les termes de « données de santé à caractère personnel » dans le premier alinéa de l'article L.1111-8. Ce terme est également repris à l'article R. 1111-9 du même Code concernant l'hébergement des données de santé.

108. Les données de santé sont des éléments qui font référence à un individu et qui permettent de tirer une information sur son état de santé. La lecture combinée de l'arrêt CJCE du 6 novembre 2003, affaire C-101/03 *Lindqvist* et l'avis 4/2007 sur le concept de données de santé du groupe de travail de « l'article 29[320] » nous indique que les données de santé doivent être abordées avec « une interprétation large de sorte qu'elles comprennent des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne ». Il convient de mettre en lumière la différence de sens et de portée des notions d'information et de donnée.

Comme exposé précédemment, l'information est un contenant, il convient donc de se pencher sur son contenu. L'information est exploitable seulement si plusieurs messages sont rassemblés. Selon H. Romeyer[321], les données sont la forme codée de l'information en vue d'un traitement déterminé. La donnée est la représentation résiduelle d'une information, elle est conventionnelle afin de pouvoir être traitée ou interprétée plus facilement et par plusieurs systèmes. Cette analyse permet de constater qu'une information est collectée alors que les données sont traitées pour en tirer une information.

La donnée est un élément technologique de l'information. En d'autres termes, une donnée isolée n'est qu'une partie d'une information inconnue. La somme de plusieurs données aboutira à les transformer, les assembler en un seul contenant : l'Information. A titre d'exemple, si l'on recueille plusieurs données : douleurs vives + épaule gauche + difficultés à respirer + sensation « de barre » ventrale + perte de connaissance ; l'information est une probabilité d'un cas d'infarctus du myocarde auquel le médecin sera

[320] Le groupe de travail « 29 » est appelé ainsi car il fut établi en vertu de l'article 29 de la directive 95/46/CE. Ce groupe est un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont disposées à l'article 30 de la même directive ainsi qu'à l'article 15 de la directive 2002/58/CE.
[321] H. Romeyer, Enseignant-chercheur à l'université Stendhal : *Tic et santé* Vol. 2, n° 1, 2008.

confronté, en raison des symptômes énoncés. Si l'on applique ce modus operandi plus largement, en y ajoutant des données telles que l'âge, la catégorie socio professionnelle, la situation géographique etc. On peut en tirer des conclusions concernant le comportement alimentaire ou l'hygiène de vie d'une personne entraînant, par exemple, une propension au développement des maladies cardio-vasculaires.

109. La nature protéiforme des données de santé en raison de leurs finalités.- Les données administratives sont collectées par nos structures de santé via le SNIIRAM qui centralise les données nécessaires à l'ouverture des droits au remboursement et à la gestion des dépenses. Ces données administratives comportent les feuilles de soins, les premières admissions dans un établissement de santé, les prises en charge, les données opérationnelles de routine, les conditions d'assurance et les données financières y afférant. Le contenu de ces données administratives est approuvé par un arrêté ministériel prévu à l'article L. 161-28-1 du Code Sécurité Sociale[322]. Ces données comportent donc des données sensibles à caractère médical. C'est au travers de cette centrale qu'est la SNIIRAM que le traitement automatisé devra s'effectuer.

L'article 25 de la loi «Informatique et Libertés» dispose que le traitement « automatisé » est exclu, selon le type d'informations en jeu : les traitements de « données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements » ou encore, sont interdits les traitements automatisés qui « du fait de leur nature, de leur portée ou de leurs finalités, risquent d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ». La finalité du traitement apparaît comme déterminante dans l'autorisation de traitement automatisé des données de santé à caractère personnel notamment lorsqu'il s'agit de « l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les

[322] Il est créé un système national d'information inter-régimes de l'assurance maladie qui contribue : 1° A la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par nature de dépenses, par catégorie de professionnels responsables de ces dépenses et par professionnel ou établissement ; 2° A la transmission en retour aux prestataires de soins d'informations pertinentes relatives à leur activité et leurs recettes, et s'il y a lieu à leurs prescriptions ; 3° A la définition, à la mise en œuvre et à l'évaluation de politiques de santé publique.

finalités correspondent à des intérêts publics différents », « l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes. ».

La loi «Informatique et Libertés» autorise donc le croisement d'informations détenues par différents prestataires ou institutions via un traitement automatisé des informations, sous réserve de l'accord délivré par la CNIL, et lorsqu'il s'agit d'assurer le bon fonctionnement d'un système ou lorsque ce traitement est effectué pour le compte de l'Etat[323]. C'est l'objet de la mise en place de référentiels généraux de sécurité[324] permettant le déploiement de l'Identifiant National de Santé (INS) qui est actuellement à l'étude par l'ASIP Santé et qui vise à attribuer un code unique à chaque titulaire d'un dossier médical.

110. Si l'on se penche sur le contenu du dossier médical d'un patient, on trouve des éléments qui comportent des informations à caractère personnel : âge, sexe, poids etc. Or, ces informations sont couvertes et protégées par le secret médical et font l'objet d'une protection de la loi dans le Code de santé publique[325]. Il en est de même concernant l'ordonnance délivrée par le professionnel qui doit indiquer ces mêmes éléments, selon les dispositions du Code précédemment cité[326]. Si l'on fait ici un rapide comparatif avec les applications santé, le praticien et les actes qu'il effectue sont soumis à des règles strictes de déontologie médicale, dont fait parti le secret professionnel. Dans le cas où il ne respecterait pas ses obligations, le praticien serait tenu comme pénalement responsable.

Selon la Commission d'Accès aux Documents Administratifs (CADA), « les informations à caractère[327] médical sont définies comme l'ensemble des informations concernant la santé [d'une personne] détenues par des professionnels et établissements de santé, qui sont formalisées et ont contribué à l'élaboration et au suivi du diagnostic et du traitement d'une action de prévention, ou ont fait l'objet d'échanges écrits entre professionnels de santé. ».

---

[323] Article 26 de la loi n° 78-17 du 6 janvier 1978 modifiée.
[324] Le Référentiel Général de Sécurité (RGS) est créé par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
[325] Article L1111-7 du Code de santé publique.
[326] Article R4127-76 du Code de santé publique : Nom, adresse, qualité du prescripteur. - Nom, prénom, sexe et âge du malade. S'il s'agit d'un enfant, l'inscription du poids est conseillée. - la date. - la signature. - le nom des médicaments, leur posologie en chiffres, leur mode et leur condition d'administration. - la quantité prescrite ou la durée du traitement.

Ainsi, la CADA a estimé que des radiographies[328], des clichés d'IRM[329], des comptes rendus de consultations[330], des correspondances entre professionnels de santé[331], des certificats médicaux, des enregistrements vidéo de séances de thérapie, ou des enregistrements sonores de conversations téléphoniques pouvaient être communicables sous le régime des informations médicales.

111. Lorsqu'elles sont transcrites de manière brute, les données médicales se présentent sous la forme d'un bloc d'informations additionnées. Ces données brutes répertorient les bénéficiaires, les prestataires, les décomptes qui récapitulent les demandes de prise en charge et la réponse qui leur est apportée. Ces dernières sont essentiellement relevées sur les feuilles de soins et les remboursements. Depuis 2009, sont également pris en compte les soins externes hospitaliers, les facturations des cliniques, les arrêts de travail, les indemnités journalières, les maladies professionnelles ainsi que les résumés de sortie hospitaliers. Selon la CADA, les documents établis par une autorité administrative et non par un médecin, tels que les arrêtés d'hospitalisation d'office, les rapports d'enquêtes sociales ou les bilans psychologiques ne sont pas considérés comme médicaux sauf s'ils sont joints à un dossier médical[332].

On s'aperçoit, au travers de l'analyse des informations précédentes, que les données de santé couvrent un domaine au moins aussi large que les données à caractère personnel. Pour des raisons de protection des personnes physiques, il n'est pas souhaitable qu'une définition légale soit officialisée car elle pourrait conduire à diminuer le champ de protection des données de santé.

112. Enfin, selon l'Organisation Mondiale de la Santé (OMS), la santé se définit par un « état de complet bien-être physique, mental et social et ne consiste pas en une absence de maladie ou d'infirmité ». Les données de santé recouvrent donc, non seulement les pathologies, les codages des actes médicaux, les radios etc., mais, également, le bien être tel que la santé mentale et psychique. Il est donc difficile de trancher sur une définition précise de la notion de « donnée de santé » tant il est difficile d'en déterminer les supports. A ce propos, Me. P. Desmarais remarque que les informations « protéiformes jalonnent le

[328] Décision n°20070859 Séance du 8/02/2007.
[329] Décision n°20071963 Séance du 3/05/2007.
[330] Décision n°20050872 Séance du 17/02/2005.
[331] Décision n°20042830 Séance du 8/07/2004.
[332] Décision n°20062025 Séance du 11/05/2006.

parcours de soins : l'agenda du professionnel de santé, l'ordonnance, la feuille de soin, la commande à la pharmacie, l'historique des remboursements, le PMSI hospitalier, etc. L'évolution du système de santé et des outils techniques a déstabilisé cette situation simple. ».

En résumé, il convient de retenir qu'une donnée de santé est un élément technique permettant d'identifier un individu, de façon directe ou indirecte, au moyen d'un numéro d'identification ou d'un ou plusieurs éléments qui lui sont propres. Ces éléments nous permettent de retenir la notion de « données de santé à caractère personnel[333] ».

113. L'émergence de la M-santé.- Dans le cadre de notre étude, il convient de s'interroger sur les risques que comporte l'émergence de nouvelles données sensibles, notamment avec le développement des interfaces mises à disposition des « patients internautes ». Le secteur de la M-santé est en plein développement. Aux Etats-Unis, des portails santé se développent et offrent de nombreux services aux patients internautes. Ces interfaces sur l'internet proposent, par exemple, la tenue d'un dossier médical virtuel avec la possibilité d'effectuer des diagnostics par des médecins. En outre, ces services proposent aux patients d'être mis en relation avec des sociétés pharmaceutiques et ouvrent la possibilité de participer à des recherches en lien avec leur pathologie. Ce choix effectué outre-Atlantique permet de protéger le patient virtuel contre l'exploitation commerciale de ses informations[334].

114. En France, les sites à caractère médical sont soumis à des règles protectrices relatives à l'exercice de la médecine. La première règle, ayant pour objet la protection des patients internautes, est issue de l'article L.4161-1 du Code de la santé publique. L'infraction d'exercice illégal de la médecine est constituée par la réalisation de tout acte par une personne non qualifiée, c'est-à-dire tout acte dont l'exercice est réservé à un médecin. L'intervention du médecin sur internet est admise dans le cadre de la médecine[335]. C'est-à-dire que le médecin est admis dans le cadre de son rôle concernant la télésurveillance. Mais la qualification du médecin dans le cadre d'une relation

[333] Formulation de l'article L. 1111-8 du Code de la santé publique.
[334] M. Harichaux « Les sites portails santé sur Internet : quelles perspectives ? », RDSS 2000. p.697
[335] Sur les diverses significations de la télémédecine, voir M. Harichaux, « Internet pour le droit », ed, Montchrestien, Coll, HC, Janvier 2001.

médecin/« patient internaute » pose la question de savoir à quel titre il agit. Agit-il en son nom ? En tant que représentant du site personne morale ? Il se pose également la question de la relation à distance. Est-ce bien le médecin qui répond ou un collaborateur de l'entreprise ?

L'acte médical interdit est visé par l'arrêté du 6 janvier 1962 modifié. Il s'agit de l'établissement d'un diagnostic à distance. La jurisprudence interprète largement la notion de diagnostic en admettant que « l'établissement d'un diagnostic par correspondance au profit de malades déterminés »[336] puisse constituer un exercice illégal de la médecine. Ainsi, il ressort que cette infraction peut s'appliquer à tout autre moyen de communication. De plus, la constitution de l'infraction implique une « habitude ou la direction suivie ». L'habitude est constituée par l'exercice d'un diagnostic à l'égard de plusieurs patients distincts et la notion de suivi sous-entend l'action de s'occuper à plusieurs reprises ou pendant un certain temps d'un même patient. Cependant, la Haute Juridiction admet que ces actes réservés ne constituent une infraction que lorsqu'ils s'adressent à une personne déterminée. Le juge admet que les « conseils didactiques adressés à un vaste public ne tombent pas sous le coup du délit »[337].

115. D'autres services sont proposés aux patients internautes, notamment celui offert par le site « medisite.fr » qui propose au patient virtuel une mise à disposition d'un dossier médical qu'il gère lui-même et qui est protégé par le système d'authentification[338]. Ce service reprend le projet instauré par la loi Kouchner[339] mettant en place le Dossier Médical Personnel (DMP). Le site propose ce service en ces termes : « le dossier santé en ligne est un dossier créé par vous qui vous appartient. Il est destiné à vous permettre de recenser vos antécédents médico-chirugicaux et à assurer le suivi de pathologies plus spécifiques. Vous pourrez ainsi le consulter en ligne ou l'imprimer pour le présenter à un médecin quel que soit l'endroit où vous soyez dans le monde à partir du moment où vous avez accès à internet ». Il semble que ces sites souhaitent créer une sorte d'autorégulation, notamment en adoptant une position « neutre [340]» et en accord avec une certaine déontologie. En effet, lorsque l'on analyse la charte déontologique du site, on remarque

[336] Cass crim, 2 novembre 1971, bull cril. N°290.
[337] Cass crim. 7 mars 1973, JCP 197, « les grands arrêts en droit de la santé. » Dalloz. 2010.
[338] Mot de passe
[339] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé JORF du 5 mars 2002 page 4118
[340] Sur la notion de neutralité des plateformes, voir le rapport de conseil national du numérique Mai 2014 p. 12.

une réelle volonté de dispenser des conseils à but purement informatif ayant un caractère médical et ne prétendant pas réaliser une prise en charge globale à distance[341]. Le site semble effectivement respecter à la lettre la loi «Informatique et Libertés» en évitant toute confusion ou risque de responsabilité pénale ou civile en pratiquant un diagnostic à distance.

L'évolution du système de traitement informatisé des données de santé à caractère personnel nécessite donc une attention particulière en ce qui concerne le respect des libertés fondamentales comme le droit au respect de la vie privée disposé à l'article 9 du Code civil, le respect du consentement et le droit à l'information du patient disposés à l'article L. 1111-2 du Code de la santé publique. A cette nécessité s'ajoute le fait que ces informations sensibles peuvent donner lieu à un diagnostic[342]. Ce diagnostic peut, lui-même, amener à prendre une décision relative à la santé de la personne.

b) Les données faisant craindre une exclusion sociale

116. La CNIL a toujours accordé une attention particulière[343] aux données relatives au niveau social des individus afin d'évaluer si une personne est « à risque» sans que la loi «Informatique et Libertés» ne les vise spécifiquement comme « sensibles ». C'est notamment le cas des fichiers de mauvais payeurs, des listes noires ou des fraudeurs. La CNIL[344] a estimé que de telles pratiques justifiaient « la remise en perspective de sa doctrine », elle « s'interroge sur la pérennité de ses préconisations, sur l'absence de législation spécifique, ainsi que les mesures à adopter afin de préserver les libertés individuelles... La prévention du risque ne peut en effet justifier l'instauration d'une "société à deux vitesses" excluant les plus défavorisés de la protection accordée à la vie

[341] « Nous nous interdisons toute forme de consultation médicale personnalisée à distance. Par conséquent nous ne donnerons suite à aucune demande d'avis médical concernant une situation particulière. » Charte disponible sur medisite.fr

[342] On ne développera pas ici le risque, pourtant bien réel, de délivrer un diagnostic erroné.

[343] Premier exemple concret d'un avertissement de la Commission relatif à ce type de fichier : CNIL Délibération n°88-50 du 10 mai 1988 adressant un avertissement à une association gérant « une banque de données d'opposition sur chèques pour le libre usage des particuliers et des commerçants », demandant l'arrêt immédiat du fonctionnement du traitement, qui était accessible à tous, et cela sans mesure de sécurité ni de confidentialité ; R.Perray, « *Informatique, Introduction générale et champ d'application de la loi « Informatique et Libertés »,* J.Cl. Comm, fasc 274-10, mai 2016.

[344] Les listes noires - le fichage des mauvais payeurs et des fraudeurs au regard de la protection des données personnelles – CNIL. 2003.

privée et aux libertés individuelles ». C'est à l'aide de la directive 95/46 CE qu'elle a trouvé un moyen de « renforcer ses pouvoirs » à propos de ce type de « traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, en particulier ceux ayant pour finalité d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat »[345]. Cette disposition est reprise ainsi dans la « LIL » modifiée : « Sont mis en œuvre après autorisation de la Commission [...] les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire [...] Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes[346]». Ainsi, les traitements susceptibles de présenter des risques particuliers par rapport aux droits et libertés des personnes concernées doivent être examinés avant leur mise en œuvre. Et parmi eux, figurent les traitements dont la finalité est de sélectionner « les personnes pouvant bénéficier d'un droit ou prestation ou contrat »[347]. Indirectement, la collecte de données permettant de mettre en œuvre ce type de finalité entre donc dans le champ des informations bénéficiant d'une attention particulière de la part de la Commission.

Il paraît donc probable que la liste des données considérées comme sensibles puisse être élargie, notamment au profit des éléments relevant de l'intimité, de la vie privée et des données relatives aux personnes considérées comme « à risque », lorsque celles-ci sont susceptibles d'aboutir à l'exclusion d'une personne de certains droits ou services. Cet élargissement pourrait rapidement intervenir à propos des données de santé.

117. Les données biométriques.- Etymologiquement, la biométrie désigne les techniques qui permettent de mesurer le vivant : « La biométrie recouvre l'ensemble des procédés tendant à identifier un individu à partir de la « mesure » de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales. Il peut s'agir des

---

[345] Considérant 53 de la directive 95-46 Op. Cit.
[346] Article 25 - I - 4° et 7° de la « LIL » modifiée. Pour une application : CNIL délibération n°04-072 du 21 septembre 2004 à propos du traitement preventiel, utilisé par les opérateurs de téléphonie mobile pour lister les impayés, empêchant un débiteur auprès de l'un d'eux de s'abonner chez un autre opérateur. Jusque là mis en œuvre sans autorisation, la Commission a profité de la demande d'abaissement du seuil d'inscription (30€) pour appliquer l'article 25 de la loi modifiée, nécessitant dès lors une autorisation.
[347] Les listes noires. Op. Cit. loci. p 11.

empreintes digitales, de l'iris de l'œil, du contour de la main, de l'ADN ou d'éléments comportementaux (la signature, la démarche) [348]».

Les données à caractère personnel biométriques ne sont pas considérées *a priori* comme sensibles au sens de l'article 8 de la loi «Informatique et Libertés». En revanche, elles sont spécifiquement envisagées par d'autres dispositions de ce même texte. La Commission définit elle-même les systèmes biométriques comme « les applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main), de traces (ADN, sang, odeurs). »[349]. Ce type de traitement est à l'origine de l'adoption de l'article 25 8° de la loi «Informatique et Libertés» qui impose d'obtenir l'autorisation préalable de la Commission pour collecter et traiter de telles informations. C'est par l'intermédiaire du même considérant de la directive 95/46 CE, déjà exposé à l'occasion des données sur les mauvais payeurs, que la Commission a trouvé un levier pour justifier la nécessité de prévoir un régime particulier[350]. D'autres justifications permettent d'abonder dans le sens du caractère particulier des données biométriques : c'est tout d'abord le lien indéniable qui existe entre éléments de la personnalité et données biométriques. S'agissant des informations reproduisant le corps, une photographie ou une vidéo de la personne, ou encore un enregistrement de la voix, l'ensemble de ces éléments est susceptible de constituer une atteinte à la vie privée. Mais c'est surtout sous l'angle des notions de dignité humaine et du respect du corps humain, telles que les lois bioéthiques ont pu les élaborer[351], que la justification de la protection particulière applicable aux données biométriques semble la plus pertinente, sans pour autant exclure celle relative à la vie privée ou au droit de la personnalité. C'est notamment cette vision qui semble avoir été

---

[348] CNIL, Rapport d'activité 2001, page 157, La Doc. Fr., coll. Rapports Officiels, 2002.
[349] Ibidem.
[350] Article 20 – Contrôle préalable, directive Op. Cit. : « Les Etats membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre ».
[351] Lois bioéthiques : la loi n° 94-548 du 1° juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; ainsi que la loi n° 94-653 du 29 juillet 1994 et la loin° 94-654 du 29 juillet 1994 ; Loi n° 2004-800 du 6 août 2004 relative à la bioéthique.| D. 2005, « La loi relative à la bioéthique ou comment accroître l'accès aux éléments biologiques d'origine humaine », D. Thouvenin, 116. D. 2005, Droits et libertés corporels : « Panorama de la législation, de la jurisprudence et des avis des instances éthiques », J.C Galloux, H. Gaumont-Prat, p 536 ; JCP éd. G. n° 36, 4 septembre n 1996 I 3956, « Bioéthique (Législation, jurisprudence et avis des instances d'éthique) », C. Byk.

adoptée par la Chambre Sociale de la Cour de Cassation à propos de l'usage d'un système biométrique dans une décision qui semble combiner les notions de droit de la personnalité et respect du corps humain : « Une empreinte digitale, même partielle, constitue une donnée biométrique morphologique qui permet d'identifier les traits physiques spécifiques qui sont uniques et permanents pour chaque individu [...] son utilisation [...] met en cause le corps humain et porte atteinte aux libertés individuelles »[352]. Cependant, il semble que cette position ne soit pas partagée en matière d'immigration, en effet, le Conseil Constitutionnel a estimé qu'il n'y avait pas d'atteinte au respect de la dignité humaine s'il s'agissait d'une simple identification par relevé d'empreinte, et non une étude des caractéristiques génétiques[353].

118. C'est aussi le moyen de passer outre le seul consentement de la personne concernée et donc d'imposer une autorisation là où même les dérogations à l'interdiction de collecte et traitement des données sensibles prévoient spécifiquement le cas du consentement de la personne[354]. « L'image du corps est classiquement perçue sous l'angle des droits de la personnalité découlant de l'article 9 du Code civil, mais aussi par le recours aux articles 16, 16-1 et 16-2 du même code comme s'inscrivant dans le domaine du droit au respect du corps humain et essentiellement dans celui du respect de la dignité de la personne humaine »[355]. Le respect de la dignité humaine est un principe très fort[356]devant lequel la liberté de la presse doit s'incliner[357]. Les données biométriques doivent donc

[352] Cass. chbre sociale Panorama Dalloz sur la biométrie pour la date de la décision, pan 2004-2005 Dalloz 2005. | Première décision de refus TGI Paris 1° chbr soc. 19 avril 2005, « est une atteinte injustifiée aux libertés individuelles », sans autre précision ; Rev. Com. com. élec. n°10, octobre 2005, com. 164, A. Lepage, « La biométrie refoulée de l'entreprise ».
[353] QPC, 2010-25 du 16 septembre 2010, considérant 14, J.VC *empreintes génétiques.*
[354] Article 8 - II 1° de la « LIL », Op. Cit.
[355] Droits et libertés corporels, janvier 2006 décembre 2006, Panorama de J.C. Galloux et H. Gaumont-Prat, D. 2007 p 1102, partie c - l'image du corps, 1§ voir aussi 3§ et suivants. | D. 2007, n° 19 p 1284, chronique de droits et libertés fondamentaux, « A corps défendant – la protection de l'individu contre lui-même », M. D. Roman. | RTD. Civ. 1992, M. Gobert, « réflexion sur les sources du droit et les 'principes' d'indisponibilité du corps humain et de l'état des personnes », p 489
[356] Cf. Supra introduction p. 32.
[357] CE 30 août 2006 n°276 866 AJDA 2006, 1581 ; RTD Civ. 2006 736 obs. M. Hauser | CE 13 septembre 2006 n°287 530, inédit, à propos de la publication de photographies de corps et de membres mutilés ayant incité le ministère de l'intérieur à prendre un arrêté interdisant la vente du magazine pour les mineurs, ou encore de le donner ou le proposer, et même de l'exposer à la vue des enfants.

bénéficier d'une protection spécifique. Leur absence[358] de la liste des « données sensibles » s'explique par la volonté d'accorder une protection plus forte encore, il ne s'agit en aucun cas d'un oubli. Il en est de même des données concernant le code génétique qui, tout en pouvant être considérées comme des données biométriques si elles sont utilisées pour identifier une personne, bénéficient d'une protection plus générale : « Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements »[359] doivent être autorisés par la Commission. Enfin, outre les données sensibles, ce sont certains identifiants eux-mêmes qui font l'objet d'une attention particulière. La CNIL fait une remarque qui permet de se rendre compte de la portée et de l'importance des données biométriques : « Si un mot de passe a été divulgué, il est possible de le renouveler. En revanche, il est impossible de changer son empreinte digitale qui est un élément du corps humain. C'est pourquoi, le risque de « divulgation » ou de « corruption » de cette donnée est d'autant plus sensible [360]».

119. Quid des Données de santé ? (*Conclusion*)- Comme exposé précédemment, les données de santé peuvent se présenter sous diverses formes. Or, comme les données biométriques, ces informations sont issues du corps humain mais ne sont pas protégées par un régime spécifique comme les données biométriques. Les données de santé entrent dans le champ de protection des données à caractère personnel qui est le levier le plus sûr, pour le moment, en matière de protection des données de santé à caractère personnel. Cependant, ces données sont de plus en plus générées dans le quotidien des utilisateurs via des applications ou objets connectés, lesquels échappent à la protection spécifique du secret médical et ne sont pas envisagés par le Code de santé publique. La rapidité avec laquelle ces informations peuvent êtres associées à d'autres applications exige de s'interroger sur les capacités des systèmes de traitement informatique de s'adapter aux

[358] Il est à noter que des données biométriques peuvent permettre la production d'informations sensibles comme les origines. V. N. Ameziane, M. Bogard, J. Lamoril., *Principes de biologie moléculaire en biologieclinique,* Ed. Elsevier, coll. Campus Référence, 2005, page 16 et s.
[359] Article 25 I 2° de la « LIL » modifiée.
[360] CNIL, communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, *Biométrie : des dispositifs sensibles soumis à autorisation de la CNIL,* 7 avril 2011.

exigences de la loi[361]. A l'heure actuelle, deux possibilités peuvent êtres proposées en l'espèce : soit l'utilisateur confie l'enregistrement de ses informations personnelles à des services qui les croisent et il perd le contrôle de ses données personnelles ; soit l'utilisateur devient l'administrateur de ses données et interprète ses informations en faisant lui-même le croisement des informations. Ces deux situations réclament une gouvernance originale qui permettrait de profiter des savoirs que ces informations peuvent générer[362]. Cette nouvelle gouvernance devra s'effectuer « sans favoriser des phénomènes de centralisation et sans menacer la vie privée des personnes [363]». Certaines affaires ont démontré qu'il suffit de très peu d'informations pour désanonymiser par recoupement des bases de données qui paraissaient en apparence parfaitement sécurisées[364]. Nos institutions veillent à ce que ces informations, qui, non seulement permettent d'identifier directement ou indirectement une personne, mais aussi, entrainent un risque d'exclusion sociale ; ne puissent pas faire l'objet d'un traitement ni être stockées[365].

La multiplicité des sources contenant des données personnelles nécessite de s'interroger sur la capacité des moyens de traitements à effectuer un collecte neutre des informations. La neutralité de la collecte ne pouvant être possible seulement lorsque le responsable aura pris soins de définir clairement la finalité du traitement. La finalité du traitement devant être conforme à l'article 6 et suivants de la loi «Informatique et Libertés». Le responsable du traitement devra notamment respecter l'accomplissement de certaines procédures afin que la mise en œuvre du traitement des données à caractère personnel soit conforme.

---

[361] Voir infra Part. 1, Tit. 2 Ch.3, la protection spécifique des données de santé à caractère personnel.

[362]« Les plus beaux projets Big Data se trouvent pourtant dans des secteurs que l'on observe moins, mais qui nous concernent tout autant. Logistique, maintenance prédictive, recherche, santé, énergie, culture et humanitaire même » Guide du Big Data, *l'annuaire de référence à destination de l'utilisateur,* 2014/2015.

[363] D. Cardon, A quoi rêvent les algorithmes, *Nos Vies à L'heure des Big Data,* Edition Seuil, La République des Idées, Octobre 2015.

[364] En avril 2016, plus de 50 millions de données personnelles ont été dévoilées et mises en circulation, exposant les personnes concernées à diverses fraudes : http://www.cil.cnrs.fr/CIL/spip.php?article2851.

[365] Conseil Constitutionnel, Dec. °2014-412 QPC, M. Lauren « Délit de mise et conservation en mémoire informatisée des données sensibles », Comm. Com. Elec. 2015, obs. A. Debet.

Titre 2 : La neutralité de la collecte des données personnelles comme fondement de la protection des données de santé à caractère personnel

La loi «Informatique et Libertés» vise, comme principe général, une obligation de transparence lorsqu'un traitement des données personnelles doit être effectué. Ce principe de transparence du traitement se traduit par un certain nombre de formalités devant être accomplies par le responsable du traitement (Chapitre 1). Ces obligations ont évolué et ont été allégées en fonction de la nature des données traitées, mais l'allégement de ces formalités n'a pas remis en cause les obligations du responsable du traitement qui sont immuables lors de la mise en œuvre du traitement (Chapitre 2). Ces obligations sont d'autant plus impératives lorsque le traitement des données concerne des éléments relevant d'un domaine spécifique, tel que la santé, qui est encadré par le régime spécial du secret médical (chapitre 3).

Chapitre 1 : Les obligations pesant sur le responsable du traitement

Il convient d'étudier, dans un premier temps, le régime de droit commun de la déclaration préalable qui a fait l'objet d'une évolution depuis la promulgation de la loi du 6 août 2004. Elle met un terme à la prééminence et du contrôle *a priori,* notamment avec la mise en place de normes simplifiées (section 1). Cependant, le traitement de données qualifiées de « sensibles » ou présentant un risque demeurent soumises dans la plupart des cas, à une demande d'autorisation préalable auprès de la CNIL. Néanmoins, la multiplication des opérateurs en matière de traitement et d'hébergement de données de santé à caractère personnel peut être problématique lorsqu'il s'agit d'identifier le responsable du traitement (section 2).

Section 1 : Les formalités accomplies par le maître du traitement

Jusqu'à la modification de la loi «Informatique et Libertés» intervenue en 2004, il était nécessaire de distinguer deux types de responsables du traitement, et, avec eux, deux procédures différentes. Lorsque le traitement était effectué pour le compte de l'Etat, d'un établissement public, d'une collectivité territoriale ou d'une personne morale de droit privé gérant un service public, il était nécessaire de recueillir l'avis de la Commission Nationale de l'Informatique et des Libertés, et, en cas d'avis non conforme, un décret en Conseil d'Etat devait être pris. Les autres traitements étaient alors simplement soumis à déclaration auprès de la Commission et devaient comporter l'engagement d'être en conformité avec la loi. Ce double régime constituait les deux principales procédures instituées par la loi, sans compter les régimes particuliers attachés à la nature des informations traitées et celui relatif aux données sensibles.

La loi prévoyait, par ailleurs, une disposition permettant de recourir à une procédure simplifiée pour « les catégories les plus courantes de traitements à caractère public ou privé, qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés ». Ces procédures simplifiées ont été reprises par la nouvelle loi et ont été démultipliées.

Quoi qu'il en soit, la distinction entre les traitements effectués pour le compte du « secteur public » ou pour le compte du « secteur privé » opérait clairement une différence dans le régime applicable. La loi du 6 août 2004 devait mettre fin à l'intérêt de cette

distinction. C'est aussi la volonté de la directive 95/46 CE, qui, dans son article 20, n'imposait un examen préalable que pour « les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées ». A contrario, ceux ne présentant pas de tels risques pouvaient se contenter d'une déclaration simplifiée, voire être exonérés de formalité préalable. Naturellement, sur ce point, la Directive ne pouvait pas envisager les traitements relevant de la souveraineté de l'Etat. La loi définit aujourd'hui une procédure commune quel que soit le traitement : un tronc commun, puis une série de procédures particulières qui, selon la nature des données à caractère personnel ou du traitement lui-même, assouplissent ou, au contraire, alourdissent les démarches à accomplir.

120. La procédure de déclaration auprès de la CNIL.- Ce régime est essentiellement déclaratif[366]. Celui-ci, comme les demandes d'avis ou d'autorisations à la Commission Nationale de l'Informatique et des Libertés, doit comporter un nombre minimal d'informations [367]: « L'identité et l'adresse du responsable du traitement[368], ou si celui-ci n'est pas sur le territoire d'un Etat membre de l'Union Européenne[369], ces informations sont celles du représentant[370] sur le territoire Français du responsable du traitement, ceci ne faisant pas obstacle aux actions qui peuvent être introduites contre ce dernier. - La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 25[371], 26[372] et 27[373], la description générale de ses fonctions. - Le cas échéant, les

[366] Chapitre IV de la loi « Informatique et Libertés »: Formalités préalables à la mise en œuvre des traitements. - Article 22 : « les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés. » (Sauf exceptions) ; C. Castet-Renard, « Droit de l'internet ; Droit français et européen », Montchrestien, éd. Lextenso, 2012, p. 48.
[367] Article 30 I de la « LIL » Op. Cit.
[368] Articles 5 I 1° et 30 I 1°de la « LIL » modifiée Op. Cit.
[369] Article 5 I 2° de la « LIL » modifiée Op. Cit.
[370] Article 5 II de la « LIL » modifiée Op. Cit.
[371] Il s'agit principalement des traitements constitués de données sensibles, de données génétiques, de données relatives aux infractions, condamnations ou mesures de sûreté, des traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat. Ceux où figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription des personnes. Ceux qui comportent des données (appréciations) sur les difficultés sociales des personnes ou des données biométriques nécessaires au contrôle de l'identité des personnes. Ensemble de traitements qui, par ailleurs et en principe, nécessite l'autorisation de la CNIL.
[372] Les traitements mis en œuvre pour le compte de l'Etat, autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la CNIL, lorsqu'ils relèvent de la sûreté de l'Etat, la

interconnexions, les rapprochements ou toute autre forme de mise en relation avec d'autres traitements. - Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement. - La durée de conservation des informations traitées. - Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées. - Les destinataires ou catégories de destinataires habilités à recevoir communication des données. - La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit. - Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant. - Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union Européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre Etat membre de l'Union Européenne au sens des dispositions du 2° du I de l'article 5.

Il faut ajouter que tout changement[374] de ces informations après la déclaration ou l'autorisation du traitement doit être communiqué sans délai à la Commission Nationale de l'Informatique et des Libertés[375]. Il en est de même lorsque le traitement est supprimé. Enfin, la déclaration doit comporter l'engagement que le traitement satisfait aux exigences de la loi.

---

défense ou la sécurité publique - de la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

[373] L'article vise les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la CNIL, lorsque ces traitements comportent le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou sont constitués de données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. Et, par ailleurs, les traitements autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la CNIL.

[374] Article 30 II Op. Cit. La Commission emploie le terme de « toute modification substantielle », article 43 du règlement intérieur de la CNIL - délibération n°2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés, JORF n°156 du 7 juillet 2006.

[375] R.Perray, « *Informatique, Introduction générale et champ d'application de la loi « Informatique et Libertés »,* J.Cl. Comm, fasc 274-10, mai 2016.

121. Cette obligation de déclarer qui pèse sur le responsable du traitement est primordiale. En premier lieu, elle permet à la CNIL de prendre connaissance de l'existence du traitement, de la nature des données traitées et de la finalité poursuivie[376]. Par la suite, elle lui permettra de s'assurer de la conformité du traitement à la loi «Informatique et Libertés». C'est ensuite une formalité nécessaire pour que les personnes concernées puissent efficacement exercer leurs droits, en sachant qui détient leurs informations et engager, le cas échéant, la responsabilité du responsable du traitement. L'absence de cette obligation favoriserait sans aucun doute la clandestinité des traitements. La seule obligation d'informer la personne à l'occasion de la collecte de données ne saurait être suffisante. C'est pourquoi le fait de ne pas remplir « l'obligation de déclaration » est sanctionné[377] d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende ; la simple négligence est punie des mêmes peines. La condamnation peut concerner une personne morale[378] et être accompagnée de l'obligation de supprimer[379] tout ou partie des données, les membres de la Commission étant habilités à constater cette suppression. Il convient aussi de tenir compte des nouveaux pouvoirs de la Commission qui lui permettent, notamment, de prononcer des sanctions pécuniaires.

122. Comme la loi[380] le prévoit, la Commission met à disposition, sur son site[381], les moyens d'effectuer cette déclaration sur internet. Dans ce cas, un accusé de réception électronique est envoyé au déclarant[382] . Le dossier de déclaration est alors examiné. Si celui-ci est complet, un récépissé de la déclaration est envoyé sans délai. Néanmoins, si la Commission estime la demande incomplète, elle peut adresser, par voie électronique ou par

---

[376] Article 23, I Op. Cit

[377] Article 226-16 du Code pénal : Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier1978 relative à l'informatique, aux fichiers et aux libertés. ; CA Bourges, 2e ch., 11 janv. 2007 ; Rev. Com. com. élec. n°10 oct. 2007, com. n° 126, « Le délateur dénoncé... et condamné », A. Lepage.

[378] Article 226-24 du Code pénal.

[379] Article 222-22-2 du Code pénal.

[380] Article 23 I Op. Cit.

[381] Aussi nommée déclaration normale ou encore ordinaire, le formulaire en ligne invite à saisir chaque information nécessaire à la déclaration : http://www.cnil.fr/index.php?id=1974

[382] Une copie papier peut être obtenue sur demande par courrier. Article 42 du règlement intérieur de la CNIL Op. Cit.

courrier postal, les informations et documents éventuels faisant défaut. De même, si la CNIL estime que le traitement ne relève pas du régime classique de la déclaration, elle peut demander au responsable du traitement de justifier son choix ou l'inviter à accomplir la procédure adéquate imposée par la « LIL » et les normes particulières édictées par la Commission, notamment en matière de procédures simplifiées.

123. Le pouvoir d'appréciation de la CNIL.- Avant la réforme de la loi de 2004, il s'est posé la question de savoir quelle était la marge d'appréciation[383] dont disposait la CNIL à l'occasion de l'enregistrement des déclarations. Le Conseil d'Etat[384] a estimé que si la Commission pouvait examiner la régularité de la déclaration, notamment si cette dernière comportait l'engagement de conformité par rapport à la loi et les mentions obligatoires, a contrario, elle ne disposait d'aucune marge d'appréciation lorsque le dossier était complet et respectait le formalisme imposé par la loi, elle devrait donc délivrer sans délai le récépissé. Le Conseil d'Etat justifie : « La déclaration préalable est un procédé d'information de l'autorité publique qui facilite le contrôle sans pour autant permettre à l'administration, à la différence du régime d'autorisation préalable, d'exercer un contrôle a priori. L'autorité compétente se trouve en situation de compétence liée pour délivrer le récépissé du dépôt de déclaration sous réserve, d'une part, que la déclaration comprenne l'ensemble des indications et précisions exigées par les textes, et, d'autre part, que l'activité envisagée se situe bien dans le champ du régime de la déclaration ». Cette interprétation découle de la rédaction de l'ancien article 16[385] imposant à la Commission de délivrer « sans délai » le récépissé. La constitution d'un « fichier » manifestement contraire à l'ordre public pourrait toujours être interdite, au titre de la police générale selon

---

[383] R.Perray, « *Informatique, Introduction générale et champ d'application de la loi « Informatique et Libertés »,* J.Cl. Comm, fasc 274-10, mai 2016 ; DEBET, A. / MASSOT, J. / METALLINOS, N. « La protection des données à caractère personnel en droit français et européen », Informatique et Libertés coll. Les intégrales 2015, n°10, éd. Lextenso.

[384] CE, 6 janvier 1997 n° 159129, Section, Caisse d'Epargne Rhône Alpes Lyon, Publié au recueil Lebon. En l'espèce, une caisse d'épargne souhaitait créer un traitement concernant les naissances survenues sur son secteur territorial pour proposer des livrets d'épargne aux parents pour leur enfant. La décision du Conseil d'Etat intervient après deux rejets de la Commission de délivrer le récépissé de déclaration, le premier en date du 15 juillet 1993 et le second implicite suite au silence gardé ; T-X. Girardot, « *Régime de la déclaration préalable des traitements informatisés d'informations nominatives.* » AJDA 1997 p 156,

[385] Actuel article 23 I de la loi.

le Conseil d'Etat[386]. Enfin, si la Commission peut délivrer le récépissé seulement dans le cadre d'un traitement relevant de la procédure de déclaration classique et que son dossier est complet, ceci ne présume en rien du respect des droits institués par la loi, et ce, malgré l'engagement du responsable du traitement. La CNIL peut par la suite, exercer l'ensemble de ses nouveaux pouvoirs et prendre la décision qu'elle estimera adéquate. Le Conseil d'Etat a, par ailleurs, confirmé le statut de « tribunal »[387] de la Commission, au sens de l'article 6-1 de la Convention Européenne des Droits de l'Homme. Cette formalité reste, dans tous les cas, un préalable incontournable. A défaut, et en plus de s'exposer aux sanctions citées plus haut, le traitement ne peut être utilisé pour contrôler l'activité du salarié[388] et fonder un licenciement pour cause réelle et sérieuse. La question est plus sensible en droit pénal, en raison de l'appréciation souveraine par le juge de la valeur probatoire des éléments qui lui sont soumis et de la difficulté à admettre ou non le principe de loyauté de la preuve en cette matière. Ce point amène donc un développement spécifique, qui par souci didactique, ne sera pas traité à ce stade[389]. Néanmoins, il convient aussi de relever que, si un traitement n'est déclaré qu'après sa mise en œuvre, l'enregistrement de la déclaration ne saurait être rétroactif vis-à-vis des décisions qu'aurait fondées le traitement avant la déclaration. En revanche, la question de savoir si la mise en œuvre du traitement peut être faite concurremment à la déclaration, et donc avant la délivrance du récépissé, n'est pas clairement tranchée. Ainsi, la Commission précise qu'à l'occasion de la déclaration, seule la délivrance du récépissé permet la mise en œuvre du traitement. A contrario, la Cour de Cassation a estimé, à propos d'un traitement nécessitant non pas une déclaration mais l'autorisation de la CNIL, que les opérations réalisées entre la

---

[386] Analyse de la jurisprudence de 1991 à 1999 - Informatique et Libertés 1997 ; http://www.conseil-etat.fr/ce/jurispa/index_ju_aj9716.shtml.

[387] CE, juge des référés, 19 février 2008 n° 311974, inédit au recueil Lebon : « considérant que la possibilité conférée à un organisme administratif, telle la Commission nationale de l'informatique et des libertés, qui, eu égard à sa nature, à sa composition et à ses attributions, peut être qualifiée de tribunal au sens de l'article 6-1 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales », Cf. § n°6.

[388] CA, Paris, 7 mars 1997, à propos de la surveillance des appels émis par un salarié depuis l'entreprise à l'aide d'un commutateur téléphonique, dont le traitement n'a pas été déclaré. Dans le même sens : Cour Cass. chbre sociale, 6 avril 2004, n° 01-45227, au sujet de badges automatique contrôlant l'entrée et la sortie de chaque salarié dans l'entreprise, bien que les employés aient été informés de la mise en place de ce dispositif, la déclaration du traitement n'est intervenue que deux après le licenciement pour cause réelle et sérieuse d'un salarié, cause établie notamment grâce au dispositif ; Gaz. Pal. n°202, 20 juillet 2004, note J. Benrenger-Guillon et L. Maurel-Guignot. ; Cour de cassation, chbre soc., n° 98-42.090, 14 mars 2000, les salariés ayant été informés de l'écoute des conversations téléphoniques, le mode de preuve est alors valable, D. 2000 IR p 105.

[389] Voir infra *la légitimité du traitement,* Part. 1, titre 2, Ch sect 2.

demande d'autorisation et l'autorisation accordée par la Commission, étaient couvertes [390] par celle-ci. La formalité de la déclaration représente une quantité de traitements considérable, sans que puisse être établi un chiffre exact de leur nombre. Dès 2005, la CNIL a enregistré 80 677 déclarations[391], ce qui représente une augmentation de vingt pourcent par rapport à l'année 2004. Si la Commission, dans le cadre de la procédure ordinaire, n'est doté que d'un contrôle matériel des dossiers, elle doit s'assurer que ceux-ci sont bien coforme. Pour tenter de réduire le nombre de déclarations, la loi prévoit que « les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Dans ce cas, les 226 informations requises en application de l'article 30 ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres »[392]. C'est en raison de la nécessité d'alléger la quantité de travail relative à l'accomplissement des formalités préalables et pour faciliter la mise en œuvre de certains types de traitements particulièrement courants que la CNIL, comme le prévoit la loi, soumet les traitements courants à des procédures simplifiées.

124. Les déclarations simplifiées.- Les déclarations simplifiées[393] n'ont cessé d'être développées. Prévues par l'ancienne rédaction[394], la loi «Informatique et Libertés» modifiée en reprend le principe tout en renforçant le rôle de la CNIL à travers son pouvoir réglementaire[395]: « Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit et publie, après avoir reçu le cas échéant les propositions formulées par les représentants des organismes publics et privés représentatifs, des normes destinées à simplifier l'obligation de déclaration »[396]. Dans le cas où le traitement relèverait d'une de ces normes simplifiées,

---

[390] Cf. Supra p62.
[391] La CNIL a reçu 50 832 déclarations simplifiées et 35 931 déclarations normales pour l'année 2013.
[392] Article 23 II de la loi Op. Cit.
[393] C. Castet-Renard, « Droit de l'internet ; Droit français et européen », Montchrestien, éd. Lextenso, 2012. P50.
[394] Ainsi par exemple, la délibération n°85-038 du 18 juin 1985, relative au paiement du personnel autre que ceux d'un établissement public. Ce traitement n'est aujourd'hui soumis à aucune formalité, suite à un communiqué de la Commission en date du 10 juin 2004.
[395] Art. 11 de la loi Op.Cit.: Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.
[396] Article 24 I de la loi Op. Cit.

la déclaration est beaucoup plus *simple* à remplir et doit mentionner[397] « le type du traitement que l'on entend déclarer de façon simplifiée, l'identité et l'adresse du responsable du traitement, le nom de la personne et un moyen d'entrer en contact avec elle pour la CNIL pour toutes questions ou demandes de compléments d'informations ».

Actuellement, plus d'une cinquantaine de traitements sont susceptibles de faire l'objet d'une déclaration simplifiée grâce à l'adoption de normes par la CNIL ainsi, par exemple, les « traitements automatisés d'informations nominatives mis en œuvre par les communes pour la gestion de l'état civil »[398], les traitements mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux des salariés et des visiteurs, la gestion des horaires ainsi que pour la gestion de la restauration[399], ou encore les traitements relatifs à la gestion du personnel des organismes publics et privés[400]. La Commission a regroupé[401] par thèmes ces différentes normes simplifiées afin de faciliter la recherche pour le responsable du traitement de la procédure applicable. Voici la liste de ces thèmes : gestion des personnels[402], état civil, diffusion d'informations générales, fichiers de clients et de prospects, banque et finance, assurance, consultation de données cadastrales, données fiscales, gestion de la population, taxes et redevances, facturation des services, fichiers d'élèves, gestion prêts d'ouvrages, associations, gérance immobilière, communication politique, statistiques et santé.

125. Cependant, pour bénéficier d'une déclaration simplifiée, le traitement doit être strictement conforme aux finalités définies dans la norme et ne pas comporter d'autres données à caractère personnel que celles prévues. Par exemple, le fait que le traitement puisse faire l'objet d'un transfert de données hors des pays membres de l'Union

---

[397] Exemple de déclaration simplifiée en ligne sur le site internet de la Commission : http://www.cnil.fr/index.php?id=1248

[398] Norme simplifiée n°43, délibération n° 04-067 du 24 juin 2004, modifiée par la délibération n° 2005-126 du 12 mai 2005, JORF n° 149 du 28 juin 2005.

[399] Norme simplifiée n°42, délibération n° 02-001 du 8 janvier 2002. Ne pouvant concerner que l'entrée et la sortie sur le lieu de travail à l'exception des zones nécessitant un niveau de sécurité particulier. Les éléments faisant intervenir la biométrie ne peuvent pas faire l'objet d'une déclaration simplifiée ici.

[400] Norme n°46, délibération n°2005-002 du 13 janvier 2005 portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels. JORF n°295 du 20 décembre 2005, texte n° 131.

[401] Sur son site : http://www.cnil.fr/index.php?id=1198

[402] Respectivement normes n° 46, 42, 47, 51.| n° 43| n°48 | n°12, 13, 41| n°16| n°44| n°45, 49| n°31, 32|n°8 et 10| n°27, 39| n°29, 33| n°9| n°20, 21| n° 34,24,38| n°18, 19, 26| n° 50,52,53,54.

Européenne ou qu'il comporte des données sensibles ou « spécifiques »[403] peut exclure le traitement de la procédure simplifiée. Il faut ajouter que le fait de ne pas respecter les règles définies dans la norme simplifiée, y compris par négligence, est puni[404] d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende.

126. La porté du pouvoir de la CNIL.- Le pouvoir réglementaire de la CNIL est donc d'un intérêt certain pour faciliter la mise en œuvre au quotidien de traitements présentant des risques faibles au regard du droit au respect de la vie privée, de la dignité humaine et de la protection des libertés individuelles en général. La déclaration est aussi un moyen efficace de garantir l'effectivité des droits consacrés par la loi «Informatique et Libertés» tout en permettant, sans augmenter les charges du responsable du traitement, de gérer le personnel, les fichiers clients d'une entreprise ou tout autre traitement extrêmement courant et nécessaire. Cependant, ce type de traitement doit être cantonné au traitement des données les moins sensibles afin de limiter les risques de mésusages intrinsèques à la nature de ces données. C'est également la position[405] du Conseil d'Etat qui a annulé une délibération de la Commission pour excès de pouvoir. En l'espèce, la CNIL avait adopté une norme[406] simplifiée relative aux « traitements automatisés d'informations nominatives relatifs à la paie et à la gestion des personnels des personnes physiques et morales autres que celles gérant un service public ». La formulation de la norme simplifiée indiquait que plusieurs renseignements pouvaient être consignés à cette fin ; parmi eux : l'origine d'un handicap, le remboursement de prêts, avances et autres retenues sans qu'il ne soit précisé qu'il ne peut s'agir que de ceux qui sont consentis par l'employeur, ainsi que des informations relatives aux loisirs, activités sociales et logement sans qu'il soit nécessaire que ces renseignements n'aient de lien direct avec la présence du salarié dans l'entreprise. De plus, cette liste avait seulement une valeur indicative, ce qui semble contraire au sens de l'ancien article 6 de la loi, actuel article 24 I. Dès lors, des informations pouvant porter « atteinte à la vie privée et aux libertés » auraient pu être saisies. Le Conseil a envisagé l'interdiction de mettre en « mémoire des données nominatives faisant apparaître les origines raciales et les opinions politiques,

[403] Voir supra les divers types de données à caractère personnel.
[404] Article 226-16-1 A du Code de procédure pénale. Cette incrimination englobe les cas où une exonération de toute ou partie des formalités est prévue.
[405] CE. Assemblée 12 mars 1982, n° 25173, publié au recueil Lebon.
[406] Délibération du 18 mars 1980 adoptant une norme simplifiée pour les traitements automatisés d'informations nominatives relatifs à la paie et à la gestion des personnels des personnes physiques et morales autres que celles gérant un service public.

philosophiques ou religieuses ainsi que les appartenances syndicales des personnes » a annulé l'article mis en cause et comme celui-ci est indivisible de l'ensemble, il a également annulé la décision de la CNIL. Les normes simplifiées adoptées depuis énumèrent précisément la nature des données à caractère personnel pouvant alimenter le traitement en plus de sa finalité.

Malgré le développement très important de ces normes simplifiées, beaucoup estimaient, au moment de l'élaboration de la directive de 1995 et du projet de loi transposant celle-ci, que certains traitements ne nécessitaient aucune formalité préalable car ils ne présentaient aucun danger. Si le procédé n'était pas totalement méconnu de l'ancienne loi, sa révision a institué un mécanisme original pour le droit français qui a permis de dispenser le responsable du traitement des formalités préalables à la mise en œuvre du traitement.

127. La désignation d'un Correspondant Informatique et Libertés (CIL), permettant une dispense de déclaration- Mécanisme mis en place par la CNIL, cette obligation est totalement originale[407] pour notre droit. Cette pratique est originaire des Etats-Unis, et a été intégrée en bonne place dans la loi «Informatique et Libertés». Cet acteur est à la fois un moyen pour la Commission de contourner son manque de personnel face à l'explosion du nombre de ses missions et des dossiers à traiter, mais aussi, la faculté pour le responsable du traitement d'alléger les formalités préalables à la mise en œuvre de celui-ci, et, en théorie le moyen de garantir l'effectivité des droits institués par la loi pour les personnes concernées par le traitement.

128. La désignation du CIL, le principe.- Le responsable du traitement qui désigne un CIL bénéficie alors, pour la plupart des traitements qu'il souhaite mettre en œuvre, d'une dispense de déclaration[408]. En contrepartie, le Correspondant joue le rôle de « point de relais » entre le responsable, les personnes concernées par le traitement et la CNIL. La désignation d'un CIL est donc un moyen d'obtenir une dispense de formalité, tout en permettant aux personnes concernées de trouver rapidement un *correspondant* à qui s'adresser en cas de besoin, le CIL ayant la faculté, lui aussi, d'alerter la Commission en

[407] M. A. Bensoussan, « *Le Correspondant à la protection des données à caractère personnel : un maillon important de la réforme* », Gaz. Pal. n°286 12 octobre 2004.
[408] G**.** Desgens-Pasanau**,** « La protection des données personnelles », 2ème édition, Lextenso, 2012.

cas de difficultés, si aucune solution ne peut être trouvée directement avec le responsable du traitement.

129. Le contenu de la loi.- Le dispositif prévu par la loi est le suivant : « Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24 (déclaration ordinaire et normes simplifiées), sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de l'Union Européenne est envisagé. La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel[409] ». Ainsi, le transfert de données vers un Etat non membre de l'Union Européenne n'autorise pas le responsable du traitement à recourir au CIL. On peut remarquer, comme la loi l'envisage, qu'un tel correspondant «Informatique et Libertés» a d'abord été envisagé pour les entreprises, à l'instar de son homologue américain. Les Etats-Unis n'ont pas de véritable loi «Informatique et Libertés» en dehors du secteur public. Le secteur privé a mis en place le « chief privacy officer[410] » qui est, le plus souvent, un membre du personnel de l'entreprise, sans pouvoir particulier, qui a la charge de contrôler les fichiers de l'entreprise, ou, plus exactement, qui doit contrôler que ces fichiers restent confidentiels. L'Allemagne a, depuis plusieurs années déjà, recours à ce dispositif, avec la Suède ou les Pays-Bas et sont, sur ce point, une meilleure source d'inspiration de la directive 95/46 CE, que le modèle américain. Ainsi, dans le secteur privé, si cinq personnes ou plus ont comme tâche d'effectuer des traitements « automatisés » de données à caractère personnel, ou vingt personnes si ces opérations ne sont pas automatisées, alors, le responsable du traitement a l'obligation de désigner un « délégué à la protection des données ». L'obligation n'est plus conditionnée par l'effectif de personnel affecté aux tâches de traitement, si au moins l'un des traitements nécessite une autorisation préalable ou si la société a comme activité de fournir des renseignements individuels décidant l'accès ou non à un crédit, ou encore, est une société de « marketing direct »[411]. Le secteur public est, lui aussi, soumis à ce dispositif, si, au niveau fédéral, un traitement «

[409] Article 22 III de la « LIL » modifiée Op. Cit.
[410] Littéralement *Chef de la confidentialité.*
[411] Prospection commerciale consistant à adresser des offres et publicités ciblées à partir de renseignements sur les personnes, le plus souvent conservés sous forme de listing ou de base de données.

automatisé » est mis en œuvre et/ou si vingt personnes sont affectées à des traitements non automatisés. Dans les Länders, les lois «Informatique et Libertés» imposent la désignation d'un délégué dans des conditions similaires à celles du niveau fédéral. Aux Pays-Bas, tout comme en Suède, le dispositif reste optionnel mais il permet aux organisations professionnelles de désigner un délégué ou correspondant pour l'ensemble d'une branche professionnelle. Ce dispositif a rencontré un fort succès dans ces pays[412]. C'est le caractère optionnel qui a été préféré dans la Directive 95/46CE et par la loi française. La Commission nationale de l'informatique et des libertés justifie ce choix fondé sur le volontariat, qui permettrait d'obtenir de bien meilleurs résultats qu'un système obligatoire, et de distinguer les « bons élèves » de la loi «Informatique et Libertés»[413]. C'est aussi le sens du discours du président de la Commission qui mettait en avant « l'intérêt pédagogique » du dispositif durant les débats à l'Assemblée nationale, au moment du vote de la loi du 6 août 2004.

130. En France, si le responsable du traitement souhaite désigner un correspondant à la protection des données à caractère personnel (CIL), il doit le notifier à la Commission selon les conditions prévues par le décret[414] d'application de la loi «Informatique et Libertés». Effectuée « par lettre remise contre signature ou par remise au secrétariat de la commission contre reçu, ou par voie électronique avec accusé de réception qui peut être adressé par la même voie »[415], la notification doit comporter[416]:

> *« Les nom, prénom, profession et coordonnées professionnelles du responsable des traitements, le cas échéant, ceux de son représentant, ainsi que ceux du correspondant à la protection des données à caractère personnel.*

---

[412] CNIL - Etude de droit comparé sur les correspondants à la protection des données : « les organisations qui choisissent de désigner un CIL le font, en règle générale, dans un esprit d'ouverture et de sensibilisation aux questions de protection des données personnelles ; cet état d'esprit offre, a priori, de meilleures garanties de qualité de travail aux CIL que si leur désignation ne résultait que de la volonté de remplir une obligation légale sans conviction quant à sa justification. » ; Gaz. Pal. n° 286, 12 octobre 2004, B. Thore, « tableau synthétisant le régime applicable au détaché à la protection des données personnelles en France, en Allemagne, aux Pays-Bas et en Suède » ; Gaz. Pal. n° 109, 19 avril 2005 ; A. Delvoie, « le correspondant CNIL : une adaptation du « chief privacy officer' américain ? ».

[413] Ibid note précédente

[414] Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, version consolidé au 25 mars 2007 par le décret 2007- 451 du 25 mars 2007. AJDA 2005, p 2037, note Mme Frédérique Aubert.

[415] Article 42 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit.

[416] Article 43 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit.

Pour les personnes morales, la notification mentionne leur forme, leur dénomination, leur siège social ainsi que l'organe qui les représente légalement.

Lorsque le correspondant à la protection des données à caractère personnel est une personne morale, les mêmes renseignements concernant le préposé que la personne morale a désigné pour exercer les missions de correspondant.

Si la désignation est faite seulement pour certains traitements ou catégories de traitements, l'énumération de ceux-ci.

La nature des liens juridiques entre le correspondant et la personne, l'autorité publique, le service ou l'organisme auprès duquel il est appelé à exercer ses fonctions.

Tout élément relatif aux qualifications ou références professionnelles du correspondant et, le cas échéant, de son préposé en rapport avec cette fonction;

Les mesures prises par le responsable des traitements en vue de l'accomplissement par le correspondant de ses missions en matière de protection des données.

L'accord écrit de la personne désignée en qualité de correspondant est annexé à la notification. La désignation d'un correspondant à la protection des données à caractère personnel prend effet un mois après la date de réception de la notification par la Commission nationale de l'informatique et des libertés. Toute modification substantielle affectant les informations mentionnées aux 1° à 6° est portée à la connaissance de la Commission nationale de l'informatique et des libertés, dans les formes définies à l'article 42. »

131. La mission du CIL.- La désignation du correspondant doit faire l'objet d'une notification à la Commission, ce dernier doit alors, dans les trois mois, communiquer un répertoire[417] des différents traitements mis en œuvre par le responsable du traitement qui auraient fait l'objet d'une déclaration auprès de la CNIL si aucun CIL n'avait été désigné. Il incombe au responsable de[418] fournir au CIL tous les éléments lui permettant d'établir et d'actualiser régulièrement ce répertoire. Le CIL doit mettre à disposition des personnes qui en font la demande un inventaire et leur en délivrer une copie. Pour les traitements dont il est le correspondant, il traite les demandes et réclamations des personnes. Le CIL transmet alors au responsable du traitement les demandes concernant des traitements dont il n'assure

[417] Article 48 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit.
[418] Article 47 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit.

pas le contrôle. Par ailleurs, il veille au respect de la loi «Informatique et Libertés»[419], il peut faire des recommandations au responsable du traitement et doit être consulté avant la mise en œuvre de nouveaux traitements. Chaque année, il effectue un bilan des activités en lien avec sa mission et en avise le responsable du traitement. Il doit également mettre à la disposition de la Commission Nationale de l'Informatique et des Libertés son bilan. Avant de saisir la Commission, comme la loi et le décret le lui permettent[420], le CIL doit transmettre au responsable tous les manquements qu'il aurait constatés. La CNIL peut, de son côté, solliciter les observations du CIL dès qu'elle le souhaite.

La loi du 14 avril 2016 ajoute une obligation pour le CIL en matière de traitement de données de santé en imposant au responsable de traitement qu'il rende « compte chaque année à la Commission Nationale de l'Informatique et des Libertés des traitements ainsi mis en œuvre.

Les conditions dans lesquelles ces traitements peuvent utiliser le numéro d'inscription au répertoire national d'identification des personnes physiques sont définies par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés.[421]»

Cependant, si incontestablement le CIL est susceptible d'aider à la bonne application de la loi par sa proximité avec le responsable du traitement et les personnes qui sont concernées, la loi ne vise que de façon laconique la question du statut du CIL et donc des garanties d'indépendance nécessaires à sa mission. Dès lors, c'est la crédibilité même du CIL qui peut s'en trouver affaiblie. En effet, la loi et le décret d'application ne visent que très peu d'éléments relatifs au statut du CIL.

132. Le statut du CIL.- Si une déclaration d'intention affirme qu'il est chargé « d'assurer, d'une manière indépendante, le respect des obligations prévues » par la loi, c'est sans autre élément concret qui permettrait de garantir cette indépendance[422]. C'était même

[419] Article 49 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit.
[420] Article 51 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit.
[421] Article 22, V, de loi «Informatique et Libertés» modifiée par la Loi n° 2016-457 du 14 avril 2016 relative à l'information de l'administration par l'autorité judiciaire et à la protection des mineurs, JORF n°0089 du 15 avril 2016.
[422] Debet, A. / Massot, J. / Metallinos, N. « La protection des données à caractère personnel en droit français et européen », Informatique et Libertés coll. Les intégrales 2015, n°10, éd. Lextenso. p 879.

là la volonté du président de la Commission, durant les débats relatifs à la « LIL ». Le rapporteur de la loi du 6 août 2004, affirmait que le dispositif ne devait pas aboutir à un nouveau type de salarié protégé. Par conséquent, le salarié non protégé qui serait désigné « CIL » par son employeur, lui-même responsable du traitement, n'offrirait strictement aucune garantie d'indépendance vis à vis du responsable du traitement puisqu'il serait soumis par un lien de subordination. Néanmoins, la Commission pourrait être associée à la désignation du CIL en délivrant un agrément, comme il est prévu au Luxembourg. En pratique, le correspondant pourra se *protéger* derrière les deux garanties prévues par le décret d'application de la réglementation : le CIL « ne reçoit aucune instruction pour l'exercice de sa mission » [423] et il « ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions »[424]. L'employeur devra notifier par écrit les cas où il envisagerait de donner des directives à son CIL et à son subordonné. En cas des sanctions, l'employeur devra différencier celles prises à l'encontre de son salarié et les activités de celui-ci en tant que correspondant «Informatique et Libertés» pour que ce dernier puisse, rapporter les preuves lui permettant d'obtenir l'annulation des décisions le sanctionnant injustement en raison de ses fonctions de CIL. Il convient de remarquer que le décret d'application[425] prévoit que le responsable du traitement ne peut pas exercer lui-même les activités de correspondant «Informatique et Libertés» concernant ses propres traitements[426]. Cette disposition parait nécessaire car « les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission »[427]. Une des solutions envisagées par la doctrine est alors de désigner un salarié protégé pour assurer les missions du CIL. Il est certain que le statut de salarié protégé permet de préserver l'exercice des missions du CIL[428] vis à vis du pouvoir de sanction de l'employeur, cependant, le lien de subordination reste bien présent. En outre, cette solution n'est pas applicable dans la très large majorité des entreprises françaises puisqu'elles n'ont pas un nombre suffisant de

[423] Article 46 alinéa 2 du décret d'application n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
[424] Article 22 alinéa 3 de la loi modifiée
[425] Article 46 alinéa 3 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit : Le responsable des traitements ou son représentant légal ne peut être désigné comme correspondant.
[426] « La protection des données à caractère personnel en droit français et européen », Informatique et Libertés coll. Les intégrales 2015, n°10, éd. Lextenso. Op. Cit. Loci.
[427] Article 46 alinéa 4 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit.
[428] L'employeur doit informer le comité d'entreprise dans le cas où le licenciement est envisagé et il doit se conformer à la procédure d'information de l'inspecteur du travail.

salariés pour être obligées d'avoir des délégués du personnel ou des délégués syndicaux. Cependant, si des représentants sont élus, ou, lorsqu'il existe un comité d'entreprise[429] , il est intéressant d'envisager de proposer la mise en place d'un CIL dans deux circonstances : lorsqu'un projet important d'introduction de « nouvelles technologies » dans l'entreprise est envisagé, ou, si ces technologies sont « susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail »[430]. Dans ce cas, le comité d'entreprise doit être informé et consulté. C'est l'occasion pour lui de proposer la mise en place d'un correspondant «Informatique et Libertés» dans l'entreprise et que celui-ci soit désigné parmi les membres du comité. Dans ce cas, l'intérêt serait double : pour l'employeur cela représenterait une simplification des formalités à accomplir au regard de la loi «Informatique et Libertés» tout en ayant un CIL connaissant le fonctionnement interne de l'entreprise. Pour la protection des salariés, le fait que le CIL soit un membre du comité est un gage d'indépendance. Par ailleurs, le fait que le comité d'entreprise ait la possibilité[431] de constituer des commissions sur des thèmes particuliers et de consulter des experts et des techniciens appartenant à l'entreprise permet de placer le CIL dans une situation propice à recueillir[432] certains renseignements auprès d'eux. Ensuite, une telle solution pourrait également être proposée à l'employeur à l'occasion de la modification du règlement intérieur pour y intégrer une charte du bon usage de l'informatique dans l'entreprise, ou encore, à l'occasion de l'obligation de négociation annuelle prévue par le Code du travail[433]: bien que le thème des nouvelles technologies ne fasse pas partie des thèmes obligatoires, celui relatif à l'organisation du temps de travail

---

[429] CNIL, 17 octobre 2006, Délibération n° 2006-230, « Les comités d'entreprise dispensés de déclarer à la CNIL les traitements de données à caractère personnel mis en œuvre pour la gestion des activités sociales et culturelles ».

[430] Article L2323-23 du Code du travail : Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail. Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences sur chacun des sujets mentionnés au premier alinéa.

[431] Article L 2325-22 du Code du travail.

[432] Le décret d'application prévoit que « le responsable des traitements fournit au correspondant tous les éléments lui permettant d'établir et d'actualiser régulièrement une liste des traitements automatisés mis en œuvre au sein de l'établissement, du service ou de l'organisme au sein duquel il a été désigné et qui, à défaut de désignation d'un correspondant, relèveraient des formalités de déclaration prévues par les art. 22 à 24 de la loi du 6 janvier1978 susvisée. », art. 47 du décret n°2005-1309 du20 oct. 2005 pris pour l'application de la loi n°78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés.

[433] Article L2242-1 à 14 du Code du travail.

permet d'envisager d'aborder la question de l'emploi de l'outil informatique pour contrôler l'activité du salarié.

133. Qualification du CIL.- Une autre possibilité, approuvée[434] par la CNIL, est de désigner le correspondant parmi les salariés dont la position hiérarchique permet de communiquer directement avec les dirigeants de l'entreprise. Enfin, une troisième possibilité est de désigner un tiers comme correspondant, exception faite des cas où « plus de cinquante personnes sont chargées de la mise en œuvre ou ont directement accès aux traitements ou catégories de traitements automatisés pour lesquels le responsable entend désigner un correspondant à la protection des données à caractère personnel, seul peut être désigné un correspondant exclusivement attaché au service de la personne, de l'autorité publique ou de l'organisme, ou appartenant au service, qui met en œuvre ces traitements »[435]. Le tiers peut être un auxiliaire de justice, comme un avocat par exemple. Outre sa capacité de mettre ses compétences au service de l'entreprise, il permet la mise en œuvre de la « LIL » en conseillant le responsable sur le sens de celle-ci[436]. Son statut professionnel lui permet surtout d'exercer une telle mission en toute indépendance. Cependant, l'obligation de respecter le secret professionnel pourrait entrer en conflit avec la nécessité d'informer la CNIL de certains manquements. Il est certain que le statut du CIL reste une question cruciale au sein de l'entreprise. Enfin, la réglementation prévoit les modalités permettant de décharger le CIL de ses missions : lorsque la CNIL[437] constate, après avoir recueilli ses observations, que le correspondant manque aux devoirs de sa mission, elle demande au responsable des traitements de le décharger de ses fonctions. Lorsque c'est le responsable[438] du traitement qui souhaite décharger le CIL de sa mission en raison de manquements, il doit saisir « la CNIL pour avis par lettre remise contre signature, comportant toutes précisions relatives aux faits dont il est fait grief » et notifier la saisine au correspondant, par le même moyen, et doit mentionner la faculté qu'il a d'adresser ses observations à la Commission. Cette dernière dispose alors d'un mois à compter de la réception de la saisine, renouvelable une fois par décision motivée de son

---

[434] « la CNIL rend publique sa vision du correspondant Informatique et Libertés » *in* La CNIL confirme que le correspondant à la protection des données personnelles peut être un tiers extérieur à l'entreprise ou à l'administration, C. Safinia, PI et TIC, 25 novembre 2004, Legal News.

[435] Article 44 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit

[436] « La protection des données à caractère personnel en droit français et européen », Informatique et Libertés coll. Les intégrales 2015, n°10, éd. Lextenso. Op. Cit. Loci.

[437] Article 52 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit

[438] Article 53 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit.

président, pour communiquer son avis au responsable. Ce n'est qu'après celui-ci que le CIL peut être déchargé de ses fonctions. Enfin, lorsque c'est le CIL qui souhaite démissionner[439], il doit en informer la Commission par les mêmes moyens ayant permis de notifier à celle-ci sa désignation, en mentionnant les motifs de sa démission ; celle-ci prenant effet huit jours après. S'il n'est pas remplacé, le responsable du traitement dispose d'un mois pour effectuer les formalités préalables dont il avait été dispensé en désignant un Correspondant Informatique et Libertés.

Depuis la mise en place du CIL par la loi du 6 août 2004 et par l'impulsion de la Commission, ce dispositif a été approuvé car, d'après la CNIL, la France compte désormais 10.000 Correspondants Informatique et Libertés, contre 7.000 en 2010 et 4.000 en 2008. Dans son rapport d'activité pour 2011, la CNIL en comptabilisait 8.636. Cependant, les inquiétudes relatives à l'indépendance de ceux-ci ne pourront être dissipées qu'avec le temps[440].

134. Si la nécessité d'adapter au mieux le formalisme de la loi à la réalité pratique des traitements a justifié un certain assouplissement, voire une totale dispense de formalités, la loi «Informatique et Libertés» modifiée avait pour objectif de soumettre certains traitements à un formalisme beaucoup plus strict. Ce renforcement est justifié par le caractère sensible des données en cause et de la finalité de certains traitements, c'est donc le régime de l'autorisation préalable qui est consacré ici.

[439] Article 54 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit
[440] Guide du Correspondant Informatique et Libertés édition 2011.

Section 2 : Le renforcement des obligations du responsable du traitement

Afin de mettre en en lumière la nécessité de renforcer les obligations du responsable du traitement en matière de traitement, il convient d'exposer les en premier lieu le régime des autorisations préalables, qui permettent à la CNIL d'avoir connaissance et un contrôle des différents traitements (a). Ensuite, il convient d'étudier les obligations spécifiques qui pèsent sur le responsable du traitement (b) lorsqu'il envisage d'effectuer un traitement de données de santé (c).

a) Le régime des autorisations préalables et l'obligation de sécurité

135. Le régime d'autorisation relevant de la CNIL.- L'article 25 de la loi «Informatique et Libertés» dispose que les traitements « sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 »[441]. Il s'agit donc de traitements dont les données ou la finalité sont dites sensibles ou font l'objet d'une attention particulière et qui ne relèvent pas d'un autre régime d'autorisation. A compter de la réception de la demande, la Commission dispose de deux mois[442], renouvelable une fois par décision motivée de son président, pour se prononcer. A l'issue de ce délai, le silence gardé de la CNIL équivaut à un refus de celle-ci. Désireuse de faciliter la mise en œuvre de traitements nécessitant une autorisation mais poursuivant les mêmes finalités portant sur des données de même nature

[441] 1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8. - 2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements. - 3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées. - 4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire. - 5° Les traitements automatisés ayant pour objet :- l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents. - l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes. - 6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes.

[442] Article 25 III de la « LIL » modifiée Op. Cit.

et ayant les mêmes destinataires ou catégories de destinataires, la Commission peut adopter une autorisation[443] unique les concernant. Les responsables des traitements doivent alors prendre l'engagement de se conformer aux éléments décrits dans l'autorisation unique. Aujourd'hui, il existe une quinzaine de décisions d'autorisation unique. Le responsable du traitement qui en relève, en fonction des traitements qu'il souhaite mettre en œuvre, peut alors effectuer une déclaration de conformité à ces « décisions cadres » qui s'apparentent, sur la forme, aux déclarations simplifiées. Ainsi, par exemple, l'autorisation unique de mise en œuvre de « traitements automatisés de données à caractère personnel relatifs à la gestion des applications billettiques par les exploitants et les autorités organisatrices de transports publics »[444]. L'autorisation relative à la mise en œuvre de traitements permettant la gestion des fichiers de personnes à risques par les sociétés de location de véhicules[445], l'autorisation unique relative aux « radars automatiques »[446] , le traitement mis en œuvre dans le cadre de l'identification des contrevenants au Code la route et de la gestion du contentieux du recouvrement de ces infractions, ou encore, l'autorisation unique à propos des très controversés dispositifs d'alerte professionnelle[447]. En pratique, des traitements comportant des données relatives à la biométrie, à la gestion des impayés ou aux infractions peuvent être concernés par ces autorisations uniques dans des secteurs d'activités très variés.

Cette procédure d'autorisation de la Commission n'est pas la seule. Il existe, en parallèle, un certain nombre de traitements qui relèvent d'une autre procédure d'autorisation pour lesquels la CNIL joue un rôle moindre.

---

[443] Article 25 II de la « LIL » modifiée Op. Cit

[444] Délibération n° 2008-161 du 3 juin 2008, JORF n°0153 du 2 juillet 2008 page texte n° 94.

[445] Délibération n° 2006-235 du 9 novembre 2006 portant autorisation unique de mise en œuvre par les organismes de location de véhicules de traitements automatisés de données à caractère personnel ayant pour finalité la gestion de fichiers de personnes à risques, JORF n° 297 du 23 décembre 2006.

[446] Délibération n° 2006-188 du 6 juillet 2006 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion du contentieux lié au recouvrement des contraventions au Code de la route et à l'identification des conducteurs dans le cadre du système de contrôle automatisé des infractions au Code de la route, JORF n° 45 du 22 février 2007 p n° 122.

[447] Délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, JORF n° 3 du 4 janvier 2006 page texte n° 79.

136. Les traitements autorisés par arrêté ministériel ou décret pris en Conseil d'Etat.- Sont autorisés par arrêté du ou des ministres[448] compétents, les traitements intéressant la sûreté de l'Etat, la défense et la sécurité publique, ceux ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales, l'exécution des condamnations pénales ou des mesures de sûreté. Si ces traitements font intervenir des données sensibles[449] (origine raciale ou ethnique, opinions politiques etc.), alors, ils sont autorisés[450] par décret en Conseil d'Etat. Concernant l'ensemble de ces traitements, l'acte réglementaire d'autorisation peut être dispensé de publication par décret du Conseil d'Etat. Ce dernier autorise, par décret[451], les traitements mis en œuvre pour « le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public qui porte sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ». Il autorise également les traitements mis en œuvre pour le compte de l'Etat portant sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. Enfin, l'article 27 II précise que « sont autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la Commission Nationale de l'Informatique et des libertés : Les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I qui requièrent une consultation du répertoire national d'identification des personnes physiques sans inclure le numéro d'inscription à ce répertoire. ». L'alinéa 2 de l'article 25 vise les traitements « qui ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 », qui ne « donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents » et qui sont « mis en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques. ». Enfin, les alinéas 3 et 4 visent les traitements « relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer » et ceux « mis en œuvre par l'Etat ou les personnes morales

[448] Article 26 I 1° et 2° de la loi « LIL » modifiée Op. Cit. ; R.Perray, « Informatique, Introduction générale et champ d'application de la loi « Informatique et Libertés », J.Cl. Comm, fasc 274-10, mai 2016.
[449] Article 8 I de la loi « LIL » modifiée Op. Cit.
[450] Article 26 II de la loi « LIL » modifiée Op. Cit.
[451] Article 27 I 1° et 2° de la loi « LIL » modifiée Op. Cit.

mentionnées au I aux fins de mettre à la disposition des usagers de l'administration un ou plusieurs télé-services de l'administration électronique, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques. »

Si aucun de ces traitements ne peut être mis en œuvre sans que la CNIL n'ait pu rendre un avis motivé[452], cet avis n'a pas à être conforme. Il doit être publié avec l'arrêté ou le décret sur lequel il porte. Seul le sens de l'avis sera publié dans les cas où une dispense de publication de l'acte réglementaire autorisant le traitement aura été décidée par décret en Conseil d'Etat. Une fois saisie, la Commission dispose d'un délai de deux mois renouvelable une fois après décision motivée de son président à compter de la demande pour se prononcer. En cas de silence à l'issue de ce délai, l'avis est réputé favorable[453]. Cependant, la CNIL a pris soin de préciser, dans son règlement intérieur, que ce délai ne peut courir sans que les documents ou les précisions demandés aient été fournis[454].

137. Le rôle de la CNIL affaibli, évolution.- Avant la modification du régime des traitements issus du « secteur public », ces derniers étaient soumis à une demande d'avis motivé de la Commission. Si l'avis de la Commission était défavorable, « il ne pouvait être passé outre que par un décret pris sur avis conforme du Conseil d'Etat ou, s'agissant d'une collectivité territoriale, en vertu d'une décision de son organe délibérant approuvée par décret pris sur avis conforme du Conseil d'Etat »[455]. Si, dans tous les cas, la Commission ne pouvait pas empêcher la mise en œuvre du traitement, la procédure était incontestablement plus lourde en cas d'avis défavorable. Cette procédure, au moins théoriquement, avait aussi le mérite de dissuader le « secteur public » de négliger l'attention qu'il devait porter à sa demande d'avis, avec le risque d'allonger le délai nécessaire à la mise en place du traitement. Malgré la (bonne) volonté du président de la CNIL de contrôler les traitements, tous secteurs confondus. Il était affirmé, lors du vote de la loi de 2004, que le nouveau régime d'autorisation par décret du Conseil d'Etat ou arrêté ministériel n'affaiblirait pas le rôle de la Commission. On peut constater après quelques années de pratique que le législateur ou le gouvernement faisant ne tient pas souvent compte des observations et inquiétudes de la Commission ; voire d'une certaine négligence

[452] Articles 26 I et II, 27 I et II de la « LIL » modifiée Op. Cit.
[453] Articles 28 II de la « LIL » modifiée Op. Cit
[454] Article 45 du décret d'application n° 2005-1309 du 20 octobre 2005 Op. Cit.
[455] Article 15 de la loi « LIL » dans son ancienne rédaction.

quant au respect de l'obligation de solliciter l'avis de la Commission. Par exemple, l'arrêté pris par le ministre de l'intérieur en 2006 créant le traitement ELOI [456] afin de faciliter l'éloignement des étrangers en situation irrégulière, a été annulé[457] par le Conseil d'Etat, non seulement parce que sa création relevait de la procédure d'autorisation par décret du Conseil d'Etat, mais aussi en raison de l'absence de saisie pour avis de la Commission. D'autres exemples témoignent d'un certain mépris du « politique » vis-à-vis des décisions de la CNIL. Ainsi, lorsque celle-ci a refusé[458] d'autoriser la création, par certaines sociétés d'ayants droit, de traitements contenant les adresse IP des personnes soupçonnées de s'échanger, sans droit, des œuvres via les réseaux « peer to peer », le ministre de la culture a indiqué dès le lendemain de la décision, que : « l'examen de la transposition de la directive sur le droit d'auteur pourrait être l'occasion de faire évoluer le cadre juridique et de l'adapter à ce nouvel environnement ». Il s'agissait d'envisager la création par la loi d'une nouvelle « autorité administrative indépendante » qui aurait la possibilité de réaliser la collecte et le traitement des adresses IP des internautes ; traitement qui devrait non plus relever de l'autorisation de la Commission mais d'un arrêté ou d'un décret en Conseil d'Etat après avis motivé de la Commission[459]. L'introduction du correspondant «Informatique et Libertés», si elle laisse un certain nombre d'interrogations quant à l'indépendance de celui-ci, va aussi dans le sens d'un assouplissement du formalisme exigé par la loi, tout en instaurant un acteur au plus près de là où est mis en œuvre le traitement et donc des personnes concernées par lui, au moins dans le cas des traitements relatifs au personnel de l'entreprise. Il s'agit là de la véritable justification de ces formalités préalables. Elles permettent, le moment venu, d'identifier les responsables des traitements et tendent à l'information complète des personnes concernées par eux, qui pourront prendre connaissance des finalités déclarées et des données qui les concernent. A l'exception des pouvoirs de la Commission à propos des traitements des articles 26 et 27, la nouvelle loi «Informatique et Libertés» a su s'adapter sans affaiblir le rôle des formalités préalables dans la protection. Elle est finalement un bon compromis.

---

[456] Arrêté du 30 juillet 2006 du ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire relatif à l'informatisation de la procédure d'éloignement par la création d'un traitement de données à caractère personnel au sein du ministère de l'intérieur.

[457] CE Section du contentieux, 10ème et 9ème sous-sections réunies, 12 mars 2007 n° 297888, publié au recueil Lebon ; AJDA 2007, p 560.

[458] Délibération du 18 octobre 2005.

[459] Voir les débats parlementaires au sujet de l'adoption de la loi HADOPI projet de loi, présenté le 18 juin 2008, *favorisant la* diffusion *et la* protection *de la* création *sur* internet*,* Ch. Albanel.

Cependant, ce formalisme n'est pas une fin en soi. Il est seulement un moyen de garantir que les personnes concernées par des traitements puissent valablement consentir à la collecte des données à caractère personnel la concernant. Ces principes se traduisent par un certain nombre d'obligations pesant sur le responsable du traitement, notamment en matière de données médicales ou relatives à la santé.

b) Les obligations spécifiques liées à la collecte de données de santé à caractère personnel

138. L'obligation générale de sécurité, présentation.- Elle est visée à l'article 34 de la loi «Informatique et Libertés» et dispose que le responsable du traitement est tenu de « prendre toutes les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Si le responsable du traitement ne respecte pas cette obligation, le Code pénal prévoit[460] une peine de 5 ans d'emprisonnement et de 300 000 euros d'amende. De plus, l'article 226-17 du Code pénal sanctionne le procédé de traitement, mais, également, le fait de recourir à un tiers pour effectuer le traitement. Cette infraction doit être combinée avec l'article 226-22 du même Code qui sanctionne la communication des données[461] à des tiers qui ne sont pas admis à consulter ces informations, sans autorisation expresse de la personne concernée. Un tempérament est prévu lorsque cette divulgation intervient par négligence ou imprudence : elle est punie de 3 ans d'emprisonnement et de 100 000 euros d'amende.[462]

Comme le font remarquer certains auteurs[463], on peut tout de même regretter une définition quelque peu « lapidaire » de la part du législateur, qui ne donne pas de précisions quant aux moyens employés par le responsable du traitement.

---

[460] Article 226-17 du Code pénal.
[461] Le Code vise la divulgation des données qui auraient pour conséquence de porter atteinte à la considération ou à l'intimité de la personne concernée par le traitement.
[462] *Seulement*…
[463] A. Lucas, J. Devèze, J. Frayssinet, « Droit de l'informatique et de l'internet » op.cit.loci.

139. La confidentialité présumée.- Il n'y a pas de disposition au sein de la loi de 1978 qui définisse les conditions de confidentialité. Cependant, la CNIL affirme qu'un droit à la confidentialité est présumé et découle de l'article 1 de la loi «Informatique et Libertés»[464].

140. Les garanties de confidentialité en cas de sous-traitance.- Les conditions permettant au responsable du traitement d'avoir recours à un sous-traitant sont visées à l'article 35 de loi «Informatique et Libertés». L'alinéa 1° de l'article 35 de la loi définit le sous-traitant comme « toute personne traitant des données à caractère personnel pour le compte du responsable du traitement ». Il revient au responsable du traitement de s'assurer que le sous-traitant qu'il choisit assure les garanties suffisantes pour la mise en œuvre du traitement visées à l'article 34 de la loi. La fonction du responsable du traitement est *active* en ce sens où c'est à lui qu'incombe la responsabilité de s'assurer que toutes les garanties sont assurées par le sous-traitant lors de la mise en œuvre du traitement[465]. Enfin, l'article 35 alinéa 4 de la loi «Informatique et Libertés» modifiée prévoit les conditions dans lesquelles la sous-traitance doit se dérouler : « Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement ».

141. L'obligation de sécurité visée à l'article 17 de la directive 95/46/CE[466] .- La directive européenne est, plus détaillée que la loi de 1978 «Informatique et Libertés», et

---

[464] CNIL, 5ième rapport d'activité annuel, la Doc. Fr. coll. Rapport officiels, 1982, page 131.
[465] Article 35, alinéa 3 de la loi Informatique et Libertés de 1978.
[466] 1. Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.
Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.
2. Les États membres prévoient que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures.
3. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:
- le sous-traitant n'agit que sur la seule instruction du responsable du traitement,

servait de référence à la Commission[467] avant même la modification intervenue par la loi de 2004. La directive impose plusieurs obligations au responsable du traitement : elle vise notamment les mesures techniques mais aussi organisationnelles. En effet, l'objectif de ces obligations est de garantir un niveau de confidentialité et de sécurité « approprié ». La directive anticipe toutes les étapes en obligeant le responsable du traitement à s'assurer du niveau de sécurité, que ce soit lors de la conception ou au moment de la mise en œuvre du traitement.

Il convient de remarquer que l'obligation du responsable du traitement peut être variable selon les différents types de données et de traitements. En effet, l'article 17, 1) alinéa 2 de la directive prend en compte « l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger ». L'article 17 reprend l'article 7 de la convention 108 de 1981 qui dispose que des mesures spécifiques de sécurité doivent être prises eut égard à la « fonction spécifique du fichier [468]» ainsi qu'en fonction de sa « vulnérabilité[469] ».

142. Obligation de traçabilité.- Enfin, l'article 17, 4°) de la directive 95/46/CE oblige le responsable du traitement à consigner les mesures de sécurité qui ont été mises en œuvre. Cette exigence se trouve également à l'alinéa 3 de l'article précité : le sous-traitant est tenu contractuellement de décrire toutes les mesures qu'il a mises en place afin d'assurer la sécurité visé à l'article 17. Cette obligation ne s'applique qu'entre les signataires du contrat (entre le maître du traitement et le sous-traitant) afin de pouvoir dégager la responsabilité de chacun dans la chaîne de contrat. Ainsi, la CNIL a adressé un avertissement à un hébergeur de données de santé sur le fondement du caractère déloyal de la collecte de données. Dans cette affaire, l'hébergeur de données était un sous-traitant qui

---

- les obligations visées au paragraphe 1, telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci.
4. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 1 sont consignés par écrit ou sous une autre forme équivalente.

[467] CNIL, Délibération n°03-034 du 19 juin 2003 portant adoption d'une recommandation relative au stockage et à l'utilisation de carte bancaire dans le secteur de la vente à distance ; délibération n°03-054 du 27 novembre 2003 portant avis sur les dispositions relatives au développement de l'administration électronique de l'avant projet de loi habilitant le gouvernement à simplifier le droit par voie d'ordonnance.

[468] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, le 28 janvier 1981, Rapport explication, page 10.

[469] Ibidem.

n'avait pas respecté les dispositions de l'article L1111-8 du Code de santé publique imposant à l'hébergeur de respecter la procédure d'agrément[470].

143. La nature de l'obligation de sécurité.- L'obligation de sécurité revêt, non seulement un caractère préventif, mais elle renvoie également aux « règle[s] de l'art appropriées et évolutives »[471]. Cette règle permet d'affirmer que l'obligation de sécurité est une obligation de moyens[472] . Cependant, tant la CNIL que la jurisprudence interprètent cette obligation comme une obligation de moyen renforcée[473] ; le responsable du traitement doit tout mettre en œuvre pour faire de cette obligation une garantie. En effet, la CNIL affirme, dans sa délibération n°2012-176 du 21 juin 2012, que la responsabilité de l'organisme est engagée sur « simple constat de l'inefficacité des mesures, sans considération de faute »[474].

144. L'obligation de sécurité et le risque d'homonymie.- La CNIL considère que l'obligation recouvre aussi l'obligation de ne pas permettre une identification par homonymie. Cette obligation exige du responsable du traitement de s'assurer qu'il n'y a pas de similitude entre « l'état civil de la personne au nom de laquelle les renseignements ont été demandés et celui de la personne au nom de laquelle ils sont délivrés [475]». Cette position a été suivi par la jurisprudence[476] et la CNIL a été amenée a ré-affirmer sa position récemment, considérant qu'« il incombe à chaque agent habilité à exploiter les réponses apportées par le fichier central sur une personne donnée de s'assurer de la concordance

---

[470] CNIL, 9 janvier 2012, la CNIL sanctionne une déclaration mensongère d'un hébergeur de données de santé, disponible sur : http://www.cnil.fr/la-cnil/actualite/article/article/la-cnil-sanctionne-une-declaration-mensongere-dun-hebergeur-de-donnees-de-sante ; voir également Délibération n°2013-091, la CNIL prononce un avertissement à l'encontre de la société Total raffinage marketing, le 11 avril 2013.

[471] A. Lucas., J. Dévèze, J. Frayssinet, op. cit. loci.

[472] La définition prévue par l'avant projet de loi de réforme du droit des obligations de 2005 qui n'a pas été repris en 2015 prévoyait à l'article 1149 al 2 que l'obligation de moyen constituait le fait que le « débiteur est seulement tenu d'apporter les soins et diligences normalement nécessaires pour atteindre un certain but ».

[473] CE, 15 octobre 2014, n°358876 recueil Lebon.

[474] Voir dans le même sens, CNIL, délibération n°04-051 du 3 juin 2004 portant avertissement à la Caisse d'Epargne des Alpes.

[475] CNIL, délibération n°87-69 du 7 juillet 1987, portant avis sur la mise en œuvre par la Banque de France d'un traitement automatisé d'informations nominatives relatif à l'information de la Banque de France, des établissements de crédit et des pouvoirs publics sur les agents économiques.

[476] Cass. Crim. 19 décembre 1995, CPII, n°94-81431 : *Jurisdata* n°1995-004206 ; RJDA 1996/3, °435, obs M. Veron.

entre les éléments d'identification en sa possession sur cette personne et les réponses qu'il a reçues[477] ».

145. La garantie d'un accès limité aux données.- L'obligation de confidentialité renvoie nécessairement à la problématique de savoir *qui* peut accéder aux données. Cette obligation est visée à l'article 34 alinéa 1er de la loi «Informatique et Libertés» qui prévoit les conditions d'accès à des « tiers autorisés » ; outre les tiers autorisés[478] par loi de façon ponctuelle et limitée à accéder aux données. En dehors des autorisations encadrées par loi «Informatique et Libertés», il appartient au maître du traitement de désigner les tiers autorisés à accéder aux données. En principe, le responsable et le sous-traitant sont exclus de cette habilitation. Il semble, en effet, que la notion de tiers autorisés doit être interprétée de façon restrictive et doit s'envisager au cas par cas. Par exemple, antérieurement à la réforme de 2004, la CNIL a considéré que le bénéficiaire d'un chèque impayé ne pouvait pas être considéré comme tiers autorisé à recevoir l'incident de paiement au-delà de ce qui est prévu par loi[479]. Récemment[480], la CNIL a estimé que, dans le cadre de l'accès aux dossiers médicaux par des prestataires dont la mission était d'optimiser le codage des actes médicaux, l'habilitation d'un tiers par le responsable du traitement n'était pas recevable et que, dans ce cas, « seul le médecin chargé de l'information médicale et des personnes habilitées par l'établissement » pouvaient avoir accès aux dossiers patients pour effectuer un « éventuel recodage ». Il ressort de cette affirmation que le responsable du traitement n'est pas tenu à la seule désignation des tiers habilités, il doit également apprécier la fonction du tiers autorisé qui devra être motivée et limitée aux stricts besoins[481].

Le dernier exemple précité concernant l'accès aux données médicales par des tiers qui sont des prestataires hors cadre réglementaire est une problématique qui a été envisagée par le législateur. En effet, lors de la promulgation de la loi dite Kouchner n°2002-303 du 4 mars 2002 visant à mettre en place le Dossier Médical Personnel, le législateur a souhaité mettre

---

[477] CNIL, délibération n°2010-028, du 4 février 2010 autorisant la modification de la Banque de France des modalités de gestion du fichier central des retraits des cartes bancaires.
[478] Tels que les autorités judiciaire, auxiliaires de justice c'est-à-dire le Procureur de la République, huissiers de justice chargés de l'exécution d'une décision de justice, officiers de police judicaire dans le cadre d'une enquête de flagrance. Il peut s'agir, également, d'agents de l'administration fiscale, de la consommation et de la répression des fraudes ou de tiers disposant d'une mission de contrôle définie par la loi tels que les commissaires aux comptes.
[479] CNIL, délibération n°87-100, du 20octobre 1987, concernant la réclamation déposée contre la caisse régionale du Crédit Agricole Mutuel d'Ile de France.
[480] CNIL, courrier de clôture de la mise en demeure adressée au centre hospitalier de Saint Malo.
[481] CE, 11 avril 2014, n°355624, Inédit publié au recueil Lebon.

en place un certain nombre d'obligations concernant le traitement des données de santé à caractère personnel.

c) Le traitement des données de santé à caractère personnel

146. Préalablement à l'analyse des contrats d'hébergement, il convient de préciser que la directive 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000, reprise en droit interne par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, définit l'activité d'hébergement comme une activité de commerce électronique par laquelle une personne propose ou assure, à distance et par voie électronique, la fourniture de biens ou de services. « L'hébergement consiste à fournir des informations en ligne, des communications commerciales, des outils de recherche, d'accès et de récupération de données, des outils d'accès à un réseau de communication ou d'hébergement d'informations [482]». Il s'agit donc d'un intermédiaire technique. Dans le domaine médical, la mise en conformité des moyens de communication des données de santé tend à ce que les données traitées par les professionnels de santé soient exploitables et stockées via un hébergeur. Il n'existe pas de définition légale de l'hébergeur de données de santé. Cependant, à la lecture du Code de la santé publique, on peut déduire qu'héberger des données de santé est « le fait de déposer de telles données » auprès de personnes physiques ou morales agréées à cet effet.

147. Le contrat d'hébergement.- Le décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé, comporte une indication intéressante quant à son champ d'application puisqu'il introduit, dans le Code de la santé publique, un article R.1112-7, relatif aux établissements de santé ainsi rédigé : « les informations concernant la santé des patients sont soit conservées au sein des établissements de santé qui les ont constituées, soit déposées par ces établissements auprès d'un hébergeur agréé en application des dispositions à l'article L.1111-8 ».

L'hébergement des données de santé suppose un encadrement sécurisé, en raison de leur sensibilité. En conséquence, cet hébergement ne peut être marqué par la liberté

[482] Lexique d'information communication, DALLOZ.

contractuelle. Pour encadrer cette activité le Code de la santé publique impose un modèle de contrat minimum permettant à l'hébergeur d'être agréé.

148. La qualité d'hébergeur.- L'article R.111-13 du Code la santé publique définit les rapports entre le prestataire d'hébergement et la personne physique ou morale qui en fait la demande. La législation ne le précise pas mais il peut s'agir aussi de la personne (sujet) concernée par les données. Néanmoins, le plus souvent, ce sont les professionnels ou les établissements de santé qui font la demande d'hébergement et qui ont besoin d'externaliser la conservation de leurs données. Ces deux parties se trouvent alors dans un rapport contractuel particulier car le Code de la santé publique impose le respect de certaines clauses permettant à l'hébergeur de données d'obtenir l'agrément. Ce modèle de contrat instaure une relation particuliere entre le prestataire et l'hébergeur car le législateur permet un contrôle *a priori* des conditions générales ainsi que de la procédure d'agrément. En effet, le législateur permet de rééquilibrer, en partie, la relation contractuelle entre l'hébergeur et le bénéficiaire, lorsque la protection des personnes le nécessite ; notamment, par l'intermédiaire de clauses imposées aux deux parties.

Issu du décret du 29 avril 2002, l'article R.1111-13 du Code de la santé publique énonce neuf points qui doivent être intégrés aux modèles de contrats qui permettront à l'hébergeur de présenter sa demande d'agrément[483].

[483] Les modèles de contrats devant être joints à la demande d'agrément, mentionnés au 5° de l'article R. 1111-12, contiennent obligatoirement au moins les clauses suivantes :
1° La description des prestations réalisées : contenu des services et résultats attendus ;
2° Lorsque le contrat est souscrit par la personne concernée par les données hébergées, la description des modalités selon lesquelles les professionnels de santé et les établissements de santé les prenant en charge et désignés par eux peuvent être autorisés à accéder à ces données ou en demander la transmission et l'indication des conditions de mise à disposition de ces données
3° Lorsque le contrat est souscrit par un professionnel de santé ou un établissement de santé, la description des modalités selon lesquelles les données hébergées sont mises à leur disposition, ainsi que les conditions de recueil de l'accord des personnes concernées par ces données s'agissant tant de leur hébergement que de leurs modalités d'accès et de transmission ;
4° La description des moyens mis en œuvre par l'hébergeur pour la fourniture des services ;
5° La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, ainsi que de la périodicité de leur mesure ;
6° Les obligations de l'hébergeur à l'égard de la personne à l'origine du dépôt des données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui ;
7° Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau équivalent de garantie au regard des obligations pesant sur l'activité d'hébergement ;
8° Une information sur les garanties permettant de couvrir toute défaillance éventuelle de l'hébergeur ;

Au regard des clauses obligatoires du contrat d'hébergement, on s'aperçoit que des failles sont ouvertes concernant l'accès direct de la personne à ses informations.

L'article L.1111-7 du Code de la santé publique permet à toute personne d'accéder aux informations concernant sa santé, c'est-à-dire qu'aucun intermédiaire n'est censé se mettre entre la personne et les informations la concernant. Cependant, au visa de l'article R.1111-14 du Code de la santé publique relatif à la politique de confidentialité, on peut se poser la question de savoir si le contrat d'hébergement peut en disposer autrement.

Malgré le principe posé par l'article L.1111-7 alinéa 3[484] du Code de santé publique, on s'aperçoit qu'il n'est pas transmis un modèle de contrat mais un document qui présente la politique de confidentialité et de sécurité. Ce document a pour objet de faire apparaître « les moyens mis en œuvre pour assurer le respect des dispositions de l'article L.1111-7 » du Code de la santé publique[485]. En effet, on trouve l'exemple de modèle de contrat d'hébergement subordonnant l'accès aux informations de la personne à l'accord du professionnel ou de l'établissement de santé à l'origine du dépôt d'un dossier. Or, il faut rappeler que depuis le 1er février 2009 « l'accès aux données détenues est limité au professionnel ou à l'établissement de santé qui les a déposées, l'hébergement peut se faire sans consentement de la personne »[486]. Il apparaît donc problématique que la personne soit obligée de recourir à une action en justice pour obtenir l'autorisation d'accès à des informations à caractère médical dont elle n'est pas elle-même dépositaire, et pour lesquelles elle n'a pas donné son consentement.

Il était pourtant prévu, à l'origine, que les contrats d'hébergement de dossier médicaux expérimentaux prévoiraient un accès permanent au DMP via l'Internet par son

---

9° Une présentation des prestations à la fin de l'hébergement.

[484] Article L1111-7 du Code de santé publique : La présence d'une tierce personne lors de la consultation de certaines informations peut être recommandée par le médecin les ayant établies ou en étant dépositaire, pour des motifs tenant aux risques que leur connaissance sans accompagnement ferait courir à la personne concernée. Le refus de cette dernière ne fait pas obstacle à la communication de ces informations.

[485] Art R. 1111-4 CSP.

[486] Loi n°2007-127 du 30 janvier 2007 ratifiant l'ordonnance n°2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres de l'exercice illégal de ces professions, J.O.R.F du 1er février 2007.

gestionnaire. C'est là l'un des principaux atouts du caractère personnel de ce dossier[487] qui avait été mis en avant[488].

Outre les informations concernant la santé de la personne, on trouve également un grand nombre d'informations sociales telles que la profession, le domicile, les revenus disponibles etc. dont la plupart sont relatives à des tiers. On retrouve également ce type d'informations dans le dossier du mineur ou des personnes suivies psychiatriquement. En d'autres termes, la personne ne peut pas accéder à ses données lorsqu'elles concernent des tiers dépositaires. L'article L.1111-7 du Code la santé publique dispose que le titulaire du dossier ne peut « accéder aux informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant un tel tiers ».

Les hébergeurs de données se retrouvent dans une situation délicate en ce sens où ils ont le choix de violer soit les dispositions de l'article L.1111-7 du Code de la santé publique en ne donnant pas une réponse favorable aux demandes d'accès direct du patient, soit la disposition mentionnant qu'une personne ne peut pas accéder aux informations détenues ou recueillies auprès de tiers. La solution serait de créer un dossier social à part, en cas de prise en charge pluridisciplinaire nécessaire ou de limiter ces informations à un dossier non hébergé.

En ce qui concerne le contrôle de la production des données à caractère médical, l'article R.1111-9 du Code de la santé publique dispose que pour être en conformité, les hébergeurs doivent permettre l'identification des personnes « en charge de l'activité d'hébergement, dont un médecin, en précisant le lien contractuel qui les lie ».

La présence d'un médecin pour contrôler, trier les informations et gérer les demandes d'accès est une des conditions nécessaires pour que l'agrément soit accordé à l'hébergeur. Il convient aussi de mettre en avant le fait que les médecins ont une indépendance dans l'exercice de leur mission[489]. Le Conseil National de l'Ordre des Médecins insiste d'ailleurs sur le fait que le médecin conserve son indépendance vis-à-vis de l'hébergeur en rappelant que « les missions qui lui sont confiées doivent être exclusives de toute autre

[487] Contrat d'hébergement de DMP de Santeos, in *le dossier pharmaceutique au service du pharmacien.* M. Bertrand*,* Thèse en Pharmacie Université de Lorraine faculté de pharmacie.
[488] Loi n° 2002-303 du 4 mars 2002, op. cit.
[489] Article R4127-95 du Code de santé publique.

activité de soins, de prévention ou de contrôle dans tout organisme, quel qu'il soit »[490]. On en conclut donc que le médecin qui est recruté par l'hébergeur est tenu au secret professionnel, même vis-à-vis de son employeur.

149. Enfin, lorsque l'hébergeur transmet son dossier de demande d'agrément, il doit indiquer la manière dont le consentement de la personne a été recueilli par le professionnel ou l'établissement de santé. Malgré cette indication il faut prendre en compte la dérogation prévue par le législateur à l'article L.1111-8 du Code la santé publique issu de la loi du 30 janvier 2007 qui permet aux établissements de faire héberger les données du patient sans leur consentement[491]. En effet, le consentement peut être contourné lorsque les professionnels ou établissements de santé ont recours à leur propre système de collecte d'informations. Cependant, la loi de 2007 ne semble pas exclure le droit de rectification et le droit de suppression disposés aux articles 38 et 40 de la loi de 1978, que les informations soient déposées par la personne ou par les professionnels lors de la prise en charge. L'article 40 permet à la personne d'accéder à ses informations seulement si elles sont inexactes, équivoques ou périmées. En revanche, l'article L1110-4 du Code de la santé publique autorise le patient à s'opposer au partage d'informations le concernant entre professionnels de santé, quelle qu'en soit leur nature, dans le cadre du secret partagé. L'entreprise d'hébergement devant compter un médecin, le patient devra logiquement être informé de son droit de s'opposer au partage de ses informations.

Il convient d'ajouter le droit de « masquage » des données par le patient. Le député P.L Fagniez indique, dans son rapport de 2007[492], que le « droit de masquage » est la traduction des articles 38 et 40 de la loi «Informatique et Libertés» combinée à l'article L.1110-4 du Code de la santé publique.

Le droit de « masquage » est une faculté laissée au patient qui lui permet de ne faire figurer que les informations qu'il juge utiles dans son DMP.

---

[490] P. Cressard, *« l'actualité de notre secret médical »,* Bulletin de l'ordre des médecins, Février 2006, n°2, édito.

[491] Les professionnels et établissements de santé peuvent, par dérogation aux dispositions de la dernière phrase des deux premiers alinéas du présent article, utiliser leurs propres systèmes ou des systèmes appartenant à des hébergeurs agréés, sans le consentement exprès de la personne concernée dès lors que l'accès aux données détenues est limité au professionnel de santé ou à l'établissement de santé qui les a déposées, ainsi qu'à la personne concernée dans les conditions prévues par l'article L. 1111-7.

[492] Rapport au ministre de la santé et des solidarités, Le masquage d'informations par le patient dans son DMP, 30 janvier 2007.

Cette faculté doit être notifiée au patient et être adressée au responsable du traitement. En l'espèce, le responsable du traitement devrait logiquement être l'ASIP-Santé car c'est elle qui est chargée de s'assurer du mode d'anonymisation et de partage. Or, cette faculté de « masquage » doit avant tout faire l'objet d'une information par le coordinateur de l'équipe médicale qui s'occupe du transfert des informations. Cependant, cette faculté est souvent perçue par le praticien comme une défiance[493], car les praticiens craignent d'être tenus pour responsables en cas d'erreur médicale liée aux informations masquées. Néanmoins, la fonction de *traçage* de la Carte Profressionnel de Santé (CPS) pourra prouver qu'ils ont agi en fonction des informations auxquelles ils ont eu accès.

Il est donc nécessaire que le praticien informe le patient de son droit d'opposition et de masquage mais il devra également aviser le patient que c'est « à ses risques et périls [494]».

Durant l'exécution du contrat d'hébergement, le prestataire technique est soumis à l'inspection générale des affaires sociales. En cas de divulgation non autorisée de données de santé à caractère personnel ou en cas de manquements graves à ses obligations, notamment en matière de sécurité ou de confidentialité, la sanction sera le retrait de l'agrément de la part du Ministre de la santé. L'article R.1111.14 du Code de la santé publique dispose que, doit être joint au dossier de demande d'agrément, une explication de la politique de sécurité et de confidentialité afin d'assurer le respect des exigences de confidentialité et de secret prévues par les articles L.1110-4 et L.1111-7.

Lorsque l'on analyse les points 2 et 3 de l'article R.1111-14 du Code de la santé publique, on note que le législateur insiste sur le recueil nécessaire du consentement de la personne dont les données sont hébergées. De plus, il indique à l'article R.1111-8, dans son alinéa premier, que « l'hébergement ne peut avoir lieu qu'avec le consentement exprès de la personne concernée » or, la personne n'est pas toujours à l'origine du dépôt. Nous nous trouvons dans une relation tri-partite, en raison de l'intervention du législateur qui a pour but de savoir si les règles du consentement sont bien respectées par le cocontractant. Ce dernier a pour obligation de recueillir le consentement de la personne concernée par les données de santé recueillies en amont. Cette preuve du respect du consentement doit être portée au contrat afin que la transaction soit légalement formée.

---

[493] M. Chevillard, « *le droit de masquage par le patient dans le cadre du DMP »,* thèse en médecine générale, Université Paris VI, Pierre et Marie Curie.
[494] Article L1111-10 du Code de la santé publique.

150. Cependant, la loi du 30 janvier 2007[495] permet de passer outre le consentement de la personne concernée « dès lors que l'accès aux données détenues est limité au professionnel de santé ou à l'établissement de santé qui les a déposées, ainsi qu'à la personne concernée dans les conditions prévues par l'article L.1111-7 » du Code de la santé publique. On constate néanmoins que la dérogation peut devenir la règle dans la réalité. Or, compte tenu de l'importance du recueil du consentement du patient, il peut paraître regrettable que la règle fondatrice issue de la loi «Informatique et Libertés» concernant le consentement soit contournée en matière de traitement des données de santé lorsque celles-ci sont collectées dans le cadre d'une prise en charge.

De fait, ce qui faisait l'essence même du consentement et qui entre dans la finalité du principe de démocratie sanitaire au service du patient s'en trouve nettement modifié ou non respecté. En effet, cette disposition fait entrer le contrat dans un cadre classique qui est une relation bipartite entre l'hébergeur et l'établissement ou professionnel de santé. Les fondamentaux du droit des contrats nous amènent à fonder cette relation sur l'article 1121 du Code civil qui dispose des conditions de la stipulation pour autrui reconnue par la jurisprudence[496]. De fait, la personne dont les données sont hébergées se trouve exclue du contrôle des informations la concernant. Cette situation nous pousse donc à constater que la tierce personne au contrat dispose d'une action en responsabilité contre le promettant, laquelle peut obliger l'hébergeur à exécuter ses obligations, mais, en réalité, la personne concernée n'est pas informée des rapports qui existent entre l'hébergeur et le cocontractant.

Il convient ensuite d'analyser la procédure d'agrément permettant une exploitation normalisée des données de santé : le décret du 4 janvier 2006 dit « décret hébergeur » conformément à l'article L.1111-8 du Code de la santé publique, dispose des conditions d'agrément des hébergeurs ainsi que des informations que doivent fournir ces derniers lors de leur demande au comité d'agrément[497].

---

[495] Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n°2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions, J.O.R.F du 1er février 2007.

[496] Civ. 2ième, 17 déc. 1954. 269, note R. Rodiere; JCP 1955. II. 8490 note R. Savatier concernant une convention passée entre l'Assistance publique et le centre national de transfusion sanguine, accompagnée d'une stipulation pour autrui au profit du malade ; Civ. 1ère, 14 nov. 1995, Bull. civ. I, n°414 ; JCP 1996. I. 3985, n°7, obs. G. Viney.

[497] Art R1111-11 CSP : Le comité d'agrément mentionné à l'article R. 1111-10 comprend :

151. La procédure d'agrément.- L'agrément est délivré par arrêté du Ministère de la santé pour une durée de trois ans après l'avis du comité qui rend un avis favorable ou défavorable sur les garanties éthiques, déontologiques, financières et économiques qu'offre le candidat. En parallèle, un avis est demandé à la CNIL qui se prononce en matière de sécurité, de secret professionnel ainsi que sur les modèles de contrats, lors du dépôt de données. La CNIL examine également si les garanties sont suffisantes lorsqu'il y a une sous-traitance d'hébergement des données[498].

Néanmoins, le législateur a dû suspendre l'activité du comité en raison d'un trop grand nombre de demandes d'agrément avec la loi du 30 janvier 2007 et d'un manque d'effectif du comité. Le législateur a donc opté pour une restriction de l'activité du comité en le cantonnant aux demandes d'hébergement de DMP.

Cet agrément n'est pas réellement effectif car, en cas de refus de la part du comité, l'hébergement n'est pas interdit dès lors que l'hébergement respecte les dispositions de la loi du 6 janvier 1978 «Informatique et Libertés». Cela peut laisser perplexe vis-à-vis de la sanction qu'encourt celui qui héberge des données de santé sans agrément. De fait, on peut légitimement se demander dans quel cadre les données de santé sont réellement protégées. Ce constat rejoint la première analyse de notre introduction qui met en avant une « fuite d'informations » en raison du manque de contrôle des données médicales à caractère personnel. Le Ministère, en raison de la difficulté rencontrée par le comité, a décidé de déléguer la procédure en amont de l'agrément à l'ASIP Santé anciennement GIP-DMP après accord le 10 mars 2009 du Comité d'agrément sur la mise en place du référentiel des dossiers de constitution de demande.

En effet, lorsque l'on se réfère au dossier de demande d'agrément pour les hébergeurs[499], on s'aperçoit que l'ASIP-Santé intervient en tant que secrétaire pour les demandes faites par les hébergeurs de données. On constate que la loi ne parvient pas à être appliquée. Le

---

1° Un membre de l'inspection générale des affaires sociales nommé sur proposition du chef de l'inspection générale des affaires sociales ;
2° Deux représentants des associations compétentes en matière de santé, agréées au niveau national dans les conditions prévues à l'article L. 1114-1 ;
3° Deux représentants des professions de santé, l'un nommé sur proposition du Conseil national de l'ordre des médecins et l'autre sur proposition de l'Union nationale des professions de santé ;
4° Trois personnalités qualifiées.

[498] Art. R.1111-10 CSP.

[499] Disponible sur : www.esante.gouv.fr/services/referentiels/securite/le-referentiel-de-constitution-des-dossiers-de-demande-d-agrement-des.

Doyen G. Ripert relève que « le rôle de l'Administration grandit quand l'abondance et la succession rapide des lois détruisent la stabilité du régime légal ». Il ajoute que « les juristes s'effacent face aux technocrates qui ont seuls les connaissances nécessaires pour savoir comment il faut orienter l'économie »[500].

Ces obligations légales permettent de contrôler, en amont, les conditions générales d'hébergement des données de santé en obligeant les intermédiaires techniques à se conformer à un certain nombre d'obligations contractuelles. Néanmoins, on peut rapprocher ce modèle des exigences qu'imposait le Ministère de l'Economie et des Finances en matière de contrats d'assurance. Or, l'alinéa premier de l'article L.310-8 du Code des assurances a été abrogé en 2001 car les limitations ne permettaient pas aux professionnels de s'adapter aux évolutions du marché. On peut alors se poser la question de savoir si l'article R.1111-3 du Code de la santé publique ne pourrait pas être amené à être supprimé pour les mêmes motifs. Dans l'affirmative, il conviendra de se rapporter aux moyens de protection classiques pour assurer l'échange des informations à caractère médical.

152. Le CNOM indique, dans son livre blanc, qu'un médecin ne peut pas faire héberger les données de santé concernant ses patients auprès de prestataires industriels. En effet, cela entre en conflit avec le principe d'indépendance du praticien qui ne peut être financé par des entreprises, par exemple, des entreprises pharmaceutiques. Cependant, le Conseil fait référence à la procédure de certification instituée par la loi du 13 août 2004. Cette procédure a été diligentée par la Haute Autorité de Santé (HAS). Cette certification est effectuée à la demande du site hébergeur. Or, le CNOM souligne qu'il ne peut être reproché au médecin de ne pas avoir adhéré à un hébergeur « certifié ». Paradoxalement, le CNOM considère que le médecin joue un rôle important dans l'orientation des patients vesrdes sites « fiables ». Compte tenu des enjeux médicaux et industriels, il devrait être indispensable de soumettre les prestataires techniques en rapport avec des activités médicales à une certification ou à un recensement proche de la procédure d'agrément. La certification ou le recensement devraient notamment prendre en compte les modalités de consentement[501] au stockage des informations. En effet, le site hébergeur devrait permettre au patient d'accéder à ses informations comme le stipule la loi «Informatique et Libertés».

---

[500] G. Ripert, *Le déclin du droit*, LGDJ, 1949, n°156, *in* Données de santé et secret partagé, C. Zorn-Macrez. *Données de santé et secret partagé, pour un droit de la personne à la protection de ses données de santé partagées*. Presses universitaires de Nancy. Cit.

[501] Cf infra page 80

Pour ce faire, le praticien devrait délivrer les identifiants et mots de passe créés lors de la visite du patient. Le médecin, en l'espèce, deviendrait le responsable du traitement au sens où il devrait faire apparaître le but de la collecte des informations sur la santé du patient. Il devrait indiquer au patient qu'un certain nombre d'informations seraient partagées avec un tiers et indiquer la finalité et le rôle dudit tiers (prestataire) dans le traitement des données.

153. La réforme de la procédure d'agrément[502].- La loi du 26 janvier 2016 modifie l'article 1111-8 du Code de santé publique, notamment en matière d'hébergement externalisé et prévoit que « toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même, doit être agréée à cet effet. Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime. » La formulation de l'article étend le champ d'application de la loi lorsque le responsable du traitement a recours à un hébergeur externe qui doit nécessairement recourir à un hébergeur agréé. Il est cependant regrettable que le consentement de la personne concernée par le traitement ne soit pas expressément recueilli. En effet, le responsable du traitement est *simplement* tenu à une obligation d'information, le consentement est, de fait, présumé, comme le font remarquer Me M. Brac de la Perrière et A. Latrigue.[503]

154. De l'agrément à la certification.- Un apport qui pourrait être une solution alternative faute d'un régime spécifique de protection des données de santé est visé à l'article 204 I 5°) c) de la loi n°2016-41 qui autorise le gouvernement par voie d'ordonnance, dans un délai d'un an à « remplacer l'agrément prévu au même article L. 1111-8 par une évaluation de conformité technique réalisée par un organisme certificateur accrédité par l'instance nationale d'accréditation [504]». La nouvelle loi vise, non pas à alourdir les procédures, mais à permettre un contrôle sur la durée. La loi fait référence au

[502] La loi de modernisation de notre système de santé n°2016-41 vient d'être promulguée le 26 janvier 2016 JORF n°0022.
[503] L'usine Digitale, *Données de santé : ce que change la loi du 26 janvier 2016,* Dossier : Les Big Data, Nouvelle drogue des industries de santé.
[504] Article 204 de la loi de modernisation de notre système de santé, 24 janvier 2016, op. cit. loci.

Comité Français d'Accréditation (COFRAC) qui est un organisme certificateur qui a pour mission d'octroyer une certification de 5 ans à des organismes qui auront eux même pour mission de réaliser une évaluation et une certification des hébergeurs de données de santé pour une durée de 2 ans. Cette certification est basée sur la norme ISO 27001[505] qui permet aux entreprises de se conformer à un cahier des charges, sans pour autant émettre une nomenclature qui imposerait aux entreprises de suivre une classification méthodique des normes de sécurité.

Dans sa mise à jour des organismes agréés, l'ASIP-Santé distingue trois types de certifications :

« - L'hébergeur d'infrastructure, incluant la fourniture de l'hébergement physique ainsi que la mise en œuvre des matériels informatiques, leur maintenance, et éventuellement l'activité de sauvegardes externalisées,

- le deuxième est l'hébergement infogérance, incluant l'activité d'infogérance hors infogérance de l'application métier, et éventuellement l'activité de sauvegardes externalisées

- et enfin, les hébergeurs de données de santé, regroupant les deux premières certifications. »

Conclusion.- Cette forme de régulation va dans le sens des préconisations du Conseil National de l'Ordre des Médecins qui indique, dans son livre blanc publié en janvier 2015, que dans le domaine de la santé connectée, il est souhaitable de créer une régulation en informant les usagers sur la fiabilité des technologies[506]. Il ressort de cette analyse que, en plus des procédures accomplis, le responsable du traitement doit définir clairement la finalité afin que la personne concernée puisse appréhender la mise en œuvre du traitement.

[505] ISO/IEC 27001 – Management de la sécurité de l'information, disponible sur www.iso.org.fr

[506] CNOM, Santé Connectée. « *De la e-santé à la santé connectée* », 31 janvier 2015. https://www.conseil-national.medecin.fr/sites/default/files/medecins-sante-connectee.pdf.Voir dans ce sens A. Mendoza-Caminade, « *Big Data et données de santé : quelles régulations juridiques ?* », Rev. Lamy droit de l'immatériel n°127, 2016.

Chapitre 2 : La mise en œuvre du traitement

Le traitement des données à caractère personnel suppose l'intervention du responsable du traitement qui a pour fonction de déterminer les finalités et les moyens mis en œuvre pour le traitement. En matière de traitement de données de santé à caractère personnel, cette fonction suppose le respect de certaines règles permettant d'assurer une collecte « éthique » des données (Section 1). La collecte des données de santé à caractère personnel suppose également le respect du principe de licéité du traitement (Section 2).

Section 1 : Le principe de finalité du traitement

155. Le principe de finalité visé par l'article 6 de la loi «Informatique et Libertés» dispose que les données à caractère personnel « sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ». Ce principe est au cœur de la loi «Informatique et Libertés». C'est le principe qui permet de garantir le respect du droit à la vie privée découlant de l'article 2 de la Déclaration des Droit de l'Homme et du Citoyen de 1789. Ce principe s'applique à tous les traitements, qu'ils soient publics ou privés.

156. La détermination de la finalité du traitement.- Certains auteurs qualifient ce critère de « colonne vertébrale de la loi «Informatique et Libertés [507]» ». C'est à partir de la détermination de la finalité du traitement que la CNIL peut contrôler le respect des différentes obligations que doit respecter le maître du traitement. La Commission considère ainsi que la finalité du traitement doit être établie avant même la mise en œuvre du traitement[508]. La notion de finalité doit permettre, grâce à sa détermination, de mesurer la

[507] J. Frayssinet, Informatique, fichiers et libertés, Litec , 1992, n°172, ouvrage épuisé chez l'éditeur. *in* C. ZORN MACREZ op. cit. loci.
[508] CNIL, 6ième rapport d'activité, 1985, page 53. La doc. Fr. 1985.

pertinence des données traitées, leur proportionnalité, leur durée de conservation ainsi que ses destinataires[509]. La détermination de la finalité par le responsable doit permettre de comprendre de façon claire les besoins nécessaires au traitement, tant des tiers que de la personne concernée par le traitement. Cette détermination doit être effectuée au regard des conditions de légitimité visées par l'article 7 de loi «Informatique et Libertés»[510]. Le groupe de travail de « l'article 29 » précise que la « finalité doit être suffisamment précise pour permettre de déterminer quel traitement est, ou n'est pas compris » afin de permettre la « vérification de la conformité du traitement avec la loi, ainsi que l'application des garanties qui en découlent [511]». L'explicitation de la finalité doit, conformément à l'article 30 de loi «Informatique et Libertés» figurer dans la demande d'autorisation adressée à la CNIL. Les finalités doivent également figurer dans les informations à communiquer à la personne concernée par le traitement conformément à l'article 30 de loi «Informatique et Libertés». Cette obligation a fait l'objet d'une interprétation claire de la part de la CNIL qui affirme que la finalité ne doit pas être définie ni de façon trop générale ni de façon trop précise. En d'autres termes, la définition de la finalité doit permettre de recouvrir toutes les nécessités que requiert le traitement, et surtout, elle ne doit pas être « équivoque »[512]. Par exemple, le G29 considère que la définition d'une finalité visant « l'amélioration du service » ou « une offre publicitaire personnalisée » sont des finalités qui ne sont pas suffisamment précises et ne permettent pas d'apprécier la légitimité du traitement.[513] De même, dans le secteur public, la CNIL affirme que la définition de la finalité se cantonnant « à la gestion des dossiers des usagers du secteur public » ne recouvre pas la « finalité de

[509] Debet, A. / Massot, J. / Metallinos, N. « La protection des données à caractère personnel en droit français et européen », Informatique et Libertés coll. Les intégrales 2015, n°10, éd. Lextenso. p. 322.
[510] Article 7 de la loi « Informatique et Libertés » modifiée par la loi n°2004-801 du 6 août 2004 : « Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes : 1° Le respect d'une obligation légale incombant au responsable du traitement ; 2° La sauvegarde de la vie de la personne concernée ; 3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ; 4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ; 5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.
[511] G29, Avis 1/2008 du 4 avril 2008, sur les aspects de la protection des données liés aux moteurs de recherches.
[512] CNIL, 2ième Rapport d'activité, La Doc. Fr. 1978, page 80.
[513] G29, Avis 1/2008 du 4 avril 2008, op. cit. loci.

pilotage de l'activité des services[514] ». La finalité ne peut pas, pour autant, se réduire à l'explication pûrement technique d'une ou plusieurs opérations telles que le tri ou la numérisation. Un arrêt de la cour d'Appel de Versailles illustre cette interdiction dans une affaire où la déclaration de traitement pour l'organisation du contrôle des salariés ne faisait que mentionner que le système de fonctionnalité mais ne comportait pas de façon « concrète » les modalités d'utilisation[515]. Le principe de détermination de la finalité implique également que le responsable du traitement puisse anticiper les usages futurs qui pourront être fait des données collectées[516].

La finalité du traitement des données est clairement explicitée dans la norme simplifiée n°50 qui encadre la collecte et le traitement des données dans le secteur médical et paramédical[517] :

« Les traitements sont mis en œuvre pour faciliter la gestion administrative des cabinets et l'exercice des activités de prévention, de diagnostics et de soins. Ils n'assurent pas d'autres fonctions que :

- la gestion des rendez-vous ;
- la gestion des dossiers médicaux et l'édition des ordonnances ;
- la gestion et la tenue des dossiers individuels de soins ;
- l'établissement et la télétransmission des feuilles de soins ;
- l'envoi de courriers aux confrères ;
- la tenue de la comptabilité ;
- la réalisation d'études statistiques à usage interne. Les données personnelles de santé ne peuvent être utilisées que dans l'intérêt direct du patient et, dans les conditions déterminées par la loi, pour les besoins de la santé publique. Toute autre exploitation de ces données, notamment à des fins commerciales, est proscrite. La constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou

[514] CNIL, Délibération n°2005-038 du 10 mars 2005, relative à la modification du traitement « ANAISS » destiné à la gestion des dossiers des usagers des services sociaux des caisses régionales d'assurance maladie et des caisses générale de sécurité sociale.
[515] CA, Versailles, 15ième chambre, 11 janvier 2007, R.G. 05-05437, inédit.
[516] « La protection des données à caractère personnel en droit français et européen », Informatique et Libertés coll. Les intégrales 2015, n°10, éd. Lextenso. p 328.
[517] CNIL, Délibération n°2005-296 du 22 novembre 2005 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet. JORF n°7 du 8 janvier 2006.

indirectement des prescriptions médicales ou des informations médicales sont interdites, dès lors que ces fichiers permettent d'identifier directement ou indirectement un professionnel de santé. »

157. L'usage ultérieur des données et la détermination des destinataires.- Le cas de l'utilisation ultérieure[518] des données est prévu par l'article 6, 2°) de loi «Informatique et Libertés». Le texte prévoit que l'utilisation future des données est autorisée dès lors que le traitement ultérieur n'est pas « incompatible » avec la finalité initiale. L'objectif de cet encadrement est de ne pas permettre une utilisation des données collectées et de leur donner une signification nouvelle ; et, surtout, le texte vise à garantir la maîtrise des données de la personne concernée par le traitement[519]. Ainsi, le Conseil d'Etat a jugé qu'une centrale rediffusant des informations sur les demandes de crédits n'était pas compatible eut égard aux risques de ré-utilisations des données contraires à la finalité initiale[520]. De même, dans le domaine médical, la CNIL autorise l'usage encadré des données en fonction de l'usage (finalité) auquel elles sont destinées :

« Afin d'assurer la continuité des soins et avec l'accord de la personne concernée, les professionnels de santé et dans les établissements de santé, les membres de l'équipe de soins, chargés de la prise en charge du patient peuvent être destinataires des données figurant dans l'application. Les personnes affectées à la gestion du secrétariat n'ont accès, dans le respect des dispositions sur le secret professionnel, qu'aux informations relatives à la gestion du cabinet et en particulier à la gestion des rendez-vous. Afin de permettre le remboursement des actes, des prestations et leur contrôle, les personnels des organismes d'assurance maladie ont connaissance, dans le cadre de leurs fonctions et pour la durée nécessaire à l'accomplissement de celles-ci, de l'identité de l'assuré, de son numéro de sécurité sociale et du code des actes effectués et des prestations servies. Outre ces données, les médecins-conseils des caisses accèdent au code des pathologies diagnostiquées dans les conditions définies à l'article L. 161-29 du code de la sécurité sociale.

Les personnels des organismes d'assurance maladie complémentaire sont destinataires, dans le cadre de leurs attributions, de l'identité de leurs assurés, de leur numéro de sécurité sociale et, sous la forme de codes regroupés, aux catégories des actes et prestations effectués. Les organismes de recherche dans le domaine de la santé et les organismes spécialisés dans

---

[518] *Ibid note 516*.
[519] G29, Document de travail concernant la surveillance des communications électroniques sur le lieu de travail, 5401/01, 29 mai 2012, WP55.
[520] CE, 12 mars 2014, n°353193, publié au recueil Lebon.

l'évaluation des pratiques de soins peuvent être destinataires de données personnelles de santé dans les conditions définies par la loi du 6 janvier 1978 modifiée. [521]*»*

158. L'appréciation de la compatibilité ultérieure, le G29.- Dans un avis concernant la limitation de finalité rendu le 2 avril 2013, le groupe de travail définit les critères d'analyse permettant d'apprécier la compatibilité de l'usage secondaire. Il ajoute que cette appréciation devra s'effectuer au cas par cas, en prenant en considération « le contexte dans lequel les données personnelles ont été collectées et les attentes raisonnables des personnes concernées quant à leur utilisation ultérieure ; la nature des données à caractère personnel et de l'impact du traitement ultérieur sur les personnes concernées ; et enfin le mesures de protection pour assurer un traitement équitable et pour éviter tout impact sur les personnes concernées. [522]»

159. Le renouvellement de l'obligation d'information des personnes concernées.- Le traitement secondaire ou complémentaire entraîne, de fait, que le responsable du traitement devra, avant même la modification du traitement, informer les personnes concernées lors du traitement initial. L'article 32 de la loi «Informatique et Libertés» vise cette obligation en disposant que cette nouvelle information devra comporter tous les éléments relatifs au traitement ultérieur. Si cette obligation d'information (nouvelle) n'est pas respectée, le traitement secondaire ou complémentaire pourra être considéré comme « déloyal [523]». De plus, conformément à l'article 38 de la loi «Informatique et Libertés», la personne concernée devra être mise en mesure d'exercer son opposition[524].

Le principe de finalité est fréquemment mis en cause, comme le montre le nombre de plaintes adressées à la CNIL[525]. La Commission considère que le détournement de finalité constitue un risque majeur pour les libertés. Le Groupe de l'article 29[526] partage cette position, c'est la raison pour laquelle il explique, dans son analyse, qu'il s'agit d'éviter que la détermination des finalités soit trop large, dans le but notamment de ne pas expliciter les finalités ultérieures dont un traitement de données personnelles pourrait faire l'objet[527]. Selon le Groupe de l'article 29, l'importance du principe de la finalité se retrouve d'ailleurs

[521] Article 4 de la norme simplifiée 50 op.cit.loci.
[522] G29, avis concernant la limitation de la finalité, adopté le 2 avril 2013, wp 203.
[523] Conseil d'Etat. Section du contentieux. Le juge des référés société Directannonces n° 319071, du 5 septembre 2008. Mentionné au recueil Lebon.
[524] CE, 5 septembre 2008 op. cit. loci.
[525] Cahiers IP n°2. CNIL « Le corps, nouvel objet connecté » op. cit. loci.
[526] Groupe de l'article 29, avis n° 03/2013, 2 avr. 2013, WP 203.
[527] Groupe de l'article 29, avis n° 03/2013, 2 avr. 2013, WP 203.

particulièrement en matière de collecte de données massives ou « big data[528] ». Il s'agirait même d'une condition préalable et nécessaire pour l'application des différents critères de qualité de données à caractère personnel, y compris l'adéquation, la pertinence, la proportionnalité et l'exactitude des données collectées, ainsi que les conditions relatives à la durée de conservation des données[529].

160. La durée de conservation.- La finalité du traitement détermine la durée de conservation de ces informations. Le raisonnement est simple : une fois la finalité atteinte, la conservation des données n'est plus justifiée. Par exemple, dans le domaine de la santé, il convient de se rapporter à la norme simplifiée n°50 relative aux traitements des données à caractère personnel mise en œuvre dans le milieu médical et paramédical[530]. L'article 5 de la norme vise la durée de conservation en indiquant que : « les informations enregistrées ne peuvent être conservées dans l'application au-delà d'une durée de cinq ans à compter de la dernière intervention sur le dossier du patient. A l'issue de cette période, elles sont archivées sur un support distinct et peuvent être conservées pendant quinze ans dans des conditions de sécurité équivalentes à celles des autres données enregistrées dans l'application.
Les doubles des feuilles de soins électroniques doivent être conservées quatre-vingt-dix jours conformément à l'article R. 161-47 du code de la sécurité sociale. ».

Le principe de finalité impose, dans la pratique, que le responsable du traitement définisse clairement la finalité du traitement poursuivie. Cette obligation implique, de fait, que le responsable anticipe son application pour des utilisations futures du traitement des données. La loi «Informatique et Libertés» dispose que les données ne peuvent être « traitées ultérieurement de manière incompatible avec les finalités » déterminées initialement. La finalité du traitement impose au responsable de prendre en compte la qualité des destinataires. De même, la modification ou l'extension de la finalité du traitement doit faire l'objet d'une déclaration à la CNIL, selon les procédures adaptées. Le

[528] Les big data, littéralement les grosses données, est une expression anglophone utilisée pour désigner des ensembles de données qui deviennent tellement volumineux qu'ils en deviennent difficiles à travailler avec des outils classiques de gestion de base de données ou de gestion de l'information.
[529] Soltani S. « « Big data » et le principe de finalité », RLDI 2013/97, no,3233.
[530] CNIL, Délibération n°2005-296 du 22 novembre 2005 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet. JORF n°7 du 8 janvier 2006.

responsable du traitement devra accomplir des formalités complémentaires si nécessaire. Une exception est toutefois prévue pour les traitements réalisés à des fins statistiques, historiques ou scientifiques, à condition qu'un tel traitement soit effectué dans le respect des autres dispositions légales et qu'il ne soit pas utilisé pour prendre des décisions à l'égard des personnes concernées (art. 6, 2°). L'inobservation de cette obligation est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende et de 1.500.000 euros si l'infraction est commise par une personne morale. L'infraction se définit par « le fait que toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité ».[531]

A titre exemple, une dizaine d'employés d'EDF-GDF ont été condamnés pour détournement de finalité pour la vente frauduleuse à un assureur de fichiers d'abonnés. Le tribunal estimant que les employés « dans l'exercice de leurs fonctions étaient appelés à manipuler […] les informations recensées par EDF auprès de ses clients […] afin d'effectuer les opérations matérielles requises par les abonnés. Ces informations, recueillies avec cette finalité de gestion des contrats d'abonnés, ont été détournées, par les agents, de leur objet, par leur transmission, en connaissance de cause, au cabinet X, ce qui caractérise le délit visé [532]». La décision de la Cour d'Appel de Versailles du 3 mars 2003[533] offre une autre illustration intéressante. Celle-ci condamne deux autres employés du service de gestion d'EDF qui avaient, à la demande de leur avocat, produit dans un procès prud'homal des extraits du compte cotisations retraite d'un employé, obtenus par le service gérant le service spécial de retraite des électriciens. Le tribunal a sanctionné, là, le recours à ce document, considérant que « les besoins de la défense d'EDF devant les prud'hommes ne peuvent pas excuser le fait d'avoir commis sciemment ce détournement de finalité ».

Le principe de finalité semble être un principe fondamental qui doit faire l'objet d'une attention particulière, dès la saisie des informations.

---

[531] Article 226-21 du Code pénal.
[532] TGI Paris 16 déc. 1994. 17e ch. Corr. : Juris data n°1994-600554.
[533] CA, Versailles, 3 mars 2003, 7eme ch., n° 02/01715.

Section 2 : La légitimité du traitement

161. La légitimité du traitement est la notion centrale qui permet à la personne concernée par le traitement de maîtriser le contenu des informations collectées à son sujet. C'est grâce à ce principe que le droit à l'autodétermination peut être accompli et permet la reconnaissance des droits de la personne. Le principe de légitimité du traitement est visé essentiellement à l'article 7 de la loi «Informatique et Libertés». Le troisième alinéa de l'article 7 impose principalement au responsable du traitement de recueillir le consentement de la personne concernée par le traitement. Le recueil du consentement est donc requis, sauf si les conditions des cinq exceptions prévues par la loi sont remplies. Ainsi, le consentement à la collecte des données n'est pas nécessaire si « le respect d'une obligation légale » incombe « au responsable du traitement » ;

« 2° La sauvegarde de la vie de la personne concernée.

3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement.

4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci.

5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. »

Sous l'empire de l'ancienne loi, le législateur prévoyait que « toute personne physique » avait la faculté « de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement[534]. ». Selon l'ancienne rédaction, la protection avait moins de portée en ce sens où, tant que la personne n'avait pas fait valoir son droit d'opposition, le traitement pouvait avoir lieu. L'apport que représente la nécessité de recueillir le consentement de la personne est que son opposition n'est plus une faculté mais un droit. Le consentement sous-entend de faire référence à l'obligation d'information garantie par l'article 32 de loi «Informatique et Libertés» auprès de la personne concernée. Cette obligation impose au responsable du traitement de collecter et traiter les données de façon loyale.

[534]Article 26, ancien, de la loi «Informatique et Libertés», janvier 1978.

162. Le principe de loyauté.- L'essence de l'obligation de loyauté lors du traitement et de la collecte des données est le fait que le responsable du traitement ne doit pas collecter ni traiter les données à l'insu de la personne concernée[535]. La collecte de données à l'insu de la personne concernée par le traitement est donc un acte déloyal et peut constituer une atteinte à la vie privée[536]. Le principe de loyauté consiste en une information complète de la personne concernée. Un exemple illustre le fait que le défaut d'information est une atteinte à la vie privée a été jugé par Chambre Sociale de la Cour de Cassation dans l'arrêt « NIKON » où l'employeur avait mis en place un système de surveillance à l'insu de ses salariés[537].

Concrètement, une collecte transparente se définit par une information claire de la personne qui fait l'objet d'un recueil de renseignements. Le « devoir » de transparence sous-entend qu'il faut indiquer à cette personne la nature des données qui sont collectées. La nature des informations se définit par leur caractère personnel. Par exemple, le nom, le prénom, le sexe, l'adresse du domicile ou l'adresse électronique de la personne sont des informations qui relèvent de l'état civil de la celle-ci. La CNIL insiste sur le fait que ces informations revêtent un caractère sensible. De même, les coordonnées bancaires sont des éléments qui permettront une identification forte de la personne. Le principe de loyauté de la collecte d'informations est effectif par l'information de la personne qui dépose les informations qui la concernent. En pratique, le principe de loyauté s'exprime de la part du responsable du traitement par l'avertissement de l'individu. Cet avertissement implique que le responsable du traitement indique, dans la charte de confidentialité et de sécurité, le but (la finalité) dans lequel ces informations sont recueillies. D'un point de vue du fond[538],

---

[535]Article 226-18 du Code pénal. Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

[536] Cass. Crim., 3 novembre 1987, n°87-83429, Bull. Crim. 1987 n° 382 p 1007.

[537] Cour de Cassation, Chambre Sociale, Arrêt « Nikon »,2 octobre 2001, n° 99-42942, Bull. 2001 V n° 291 p233.

[538] Sur la forme, les chartes sont bien souvent indigestes et peu lisibles, de sorte que, par souci de gain de temps et pour ne pas alourdir les procédures d'inscription, le responsable du traitement ne présente pas les informations de façon évidente, ou elles ne sont pas facilement accessibles. En effet, lorsque l'on analyse les conditions générales des contrats d'adhésion de l'industriel Apple, de nombreuses clauses sont en caractères peu lisibles ou mises en forme de façon (trop) peu claire. Les conditions de fond sont réunies bien que perfectibles. Néanmoins, la personne qui dépose ses informations n'est pas informée de façon loyale car elle n'est pas mise en position de connaitre le véritable objet du contrat. Le professeur TRUDEL invite ainsi, tout particulièrement, à la prise en compte de la présentation sur les pages web des conditions de contractualisation. « Sont-elles sur un menu déroulant ? En pleine page ? En caractères suffisamment lisibles ? Quels sont les liens

le principe de loyauté n'est pas toujours respecté car l'usager ne perçoit pas toujours que ses informations sont recueillies et « peuvent faire l'objet » d'un traitement en interne et permettre un meilleur traitement de ses demandes (newsletters, offres publicitaires)[539]. Outre l'obligation d'informer la personne concernée du contenu et des moyens utilisés pour la collecte et le traitement de ses données, l'article 6 de la loi «Informatique et Libertés» impose au responsable du traitement que les données collectées soient en adéquation avec la finalité du traitement.

163. Le principe de proportionnalité.- Visé par l'article 6 de la loi, cette obligation impose que les données soient « adéquates, pertinentes et non excessive au regard des finalités pour lesquelles elles sont collectées et de leurs traitement ultérieurs ». Une décision rendue par la CNIL en 2000, sur le projet de l'Académie de Lille est un exemple qui permet d'illustrer la notion de proportionnalité du traitement. Dans cette décision, le système prévoyait un accès aux locaux de l'Académie en ayant recours à la reconnaissance des empreintes digitales. Un des arguments avancés du projet était de permettre un accès plus rapide aux bâtiments. La Commission a refusé de valider le projet au motif que « la fluidité de l'entrée du personnel ne paraissait pas justifier la constitution d'une base de données d'empreintes digitales de l'ensemble du personnel de la cité académique ».

164. La collecte directe des données.- Il convient d'aborder les obligations qui incombent aux responsables du traitement visées à l'article 32 de loi «Informatique et Libertés». En effet, l'obligation d'information est différente en termes de forme lorsque la collecte des données est faite directement auprès de la personne concernée :

- 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant.

- 2 ° De la finalité poursuivie par le traitement auquel les données sont destinées.

- 3° Du caractère obligatoire ou facultatif des réponses.

- 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse.

- 5° Des destinataires ou catégories de destinataires des données.

---

hypertextes ? ». TRUDEL P., Communication du Colloque sur Internet et le Droit, organisé par Paris I, fin 2000. Disponible sur http://www.lex-electronica.org/docs/articles_68.pdf.

[539] Voir G29, concernant la détermination de la finalité. op. cit. loci.

- 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre.

- 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne. Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.

L'article 32 de la loi impose que les différents services fassent clairement apparaître toute action visant à accéder à des informations sur l'équipement informatique, les informations qui y seront stockées ainsi que les moyens pour l'utilisateur de s'y opposer[540].

165. Les cookies.- Les cookies semblent avoir différentes fonctions : l'identification du serveur qui délivre l'information, une fonction d'horodatage et une fonction d'identification de l'utilisateur. Sur le fondement de la loi «Informatique et Libertés[541]» et de la Directive Européenne[542], il conviendrait de faire une distinction de la finalité[543] des fonctionnalités pour chaque cookie. En effet, en application du rapport du CNNum sur la notion de neutralité, il conviendrait de permettre à l'utilisateur d'avoir accès à « un nouveau choix »[544]. La problématique demeure dans la présentation de ces choix. En effet, l'utilisation des cookies par les sites ne laisse guère d'alternative à l'utilisateur en présentant directement comme suggestion de cliquer directement sur « OK » puis le formulaire électronique ajoute une indication[545] qui invite à se débarrasser de la question de savoir ce qu'implique l'utilisation des cookies. Or, au vu de la nouvelle norme 48 de la CNIL, l'information sur l'utilisation des cookies doit être produite sous forme de « cases à cocher » permettant de recueillir le consentement de l'utilisateur. Cependant, la CNIL précise que la présentation de la case « pré cochée » est contraire à l'expression d'un consentement libre et éclairé. Cette position est également validée par le Groupe de Travail

[540] Article 32 II 2°), de la loi «Informatique et Libertés» modifiée par l'ordonnance n°2011-1012 du 24 août 2011, op. cit. loci.
[541] Loi 78-17 du 6 janvier 1978 modifiée, Informatique et Libertés.
[542] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
[543] Conseil National du Numérique, « Réunir les conditions d'un environnement numérique ouvert et soutenable » mai 2014. Disponible sur :
http://www.cnnumerique.fr/wp-content/uploads/2014/06/CNNum_Rapport_Neutralite_des_plateformes.pdf.
[544] Raport du CNNum page 78, Op cit Loci.
[545] « En poursuivant votre navigation sur le site, vous acceptez l'utilisation des cookies pour vous proposer notamment des publicités ciblées en fonction de vos centres d'intérêt. »

de « l'article 29 » qui indique qu' « un consentement fondé sur l'absence d'action de la part d'une personne, par exemple dans le cas de cases précochées, ne satisfait pas aux conditions de validité du consentement[546] ». En conclusion, les méthodes actuellement employées sont inefficaces pour obtenir un consentement libre et éclairé de l'utilisateur, notamment au regard du lien hypertexte qui « suggère » à l'utilisateur que l'utilisation des cookies est normale et sans conséquences. Or, c'est précisément ce que souhaite éviter la Commission dans sa nouvelle norme n°48 : la déduction d'un profil ou d'un comportement de l'individu, « lorsque les cookies seront utilisés pour l'analyse de la navigation de l'internaute, notamment à des fins publicitaires, il faudra qu'il ait exprimé son accord[547] ». Par exemple, lorsque l'on analyse la politique d'utilisation des cookies sur le site « Medisite » on s'aperçoit que les cookies permettent « de déterminer en temps réel quelle publicité afficher sur un terminal, en fonction de sa navigation récente sur un ou plusieurs sites ou applications. » Cela semble être éloigné de la finalité du traitement mise en avant, à savoir, d'assurer le bon fonctionnement de l'utilisation de la plateforme. Il convient également de relever que le responsable du traitement est tenu, selon l'article 6 de la loi «Informatique et Libertés» et l'article 10 de la Directive Européenne, à une collecte loyale et transparente des données permettant à l'utilisateur d'être informé sur les conditions de contrôle de ses informations[548]. Il apparaît que la présentation des informations est une question fondamentale pour permettre un consentement libre et éclairé.

166. L'utilisation des cookies.- L'ordonnance n°2011-1012 du 24 août 2011 transposant la directive 2009/136/CE pose comme principe que l'utilisateur doit exprimer son consentement avant même le stockage d'informations sur l'équipement de l'utilisateur ou pour avoir accès à des informations déjà stockées, sauf si ces actions sont nécessaires à la stabilité du service ou que cette action a été expressément demandée par l'utilisateur. En d'autres termes, les traceurs[549] déposés sur l'équipement de la personne concernée par le traitement ne peuvent faire l'objet d'une utilisation que lorsque l'utilisateur a effectué une action positive exprimant son consentement. La CNIL ajoute que cette obligation s'impose

[546] Groupe de travail « article 29 » sur la protection des données, « sur la définition du consentement » adopté le 13 juillet 2011. Référence 01197/11/FR WP 187.
[547]Maitres Langlais-MPL- chroniques - « L'arme de la CNIL : les cases à cocher » 1er février 2013, disponible http://www.langlais-mpl.com/actualites/chroniques/44-l-arme-de-la-cnil-les-cases-a-cocher.html
[548] Avis du groupe de travail « article 29 » op.cit page 10.
[549] C. Castet-Renard, « Droit de l'internet ; Droit français et européen », Montchrestien, éd. Lextenso, 2012. p. 75.

« lorsque plusieurs acteurs interviennent dans le dépôt et la lecture de cookies (par exemple, lorsque les éditeurs facilitent le dépôt de cookies qui sont ensuite lus par des régies publicitaires), chacun d'entre eux doit être considéré comme coresponsable des obligations découlant des dispositions de l'article 32-II L'obligation de recueil du consentement s'impose notamment : aux éditeurs de sites, de système d'exploitation, et d'applications, aux régies publicitaires, aux réseaux sociaux, aux éditeurs de solutions de mesure d'audience. [550]»

167. La force du consentement.- Le consentement doit être spécifique, en ce sens où il doit être la représentation de la « volonté » de la personne concernée qui consent aux différents traitements. La spécificité du consentement exclut donc l'expression d'un consentement répondant à un traitement global. En d'autres termes, le consentement doit être exprimé sur les différents aspects du traitement. L'expression de la volonté de consentir doit être « détaillée » en fonction de la finalité « envisagée » ou des destinataires des données. Les travaux du Groupe de Travail de l'article 29 démontrent l'importance d'un consentement spécifique lors de la création de dossiers médicaux électroniques. En effet, le groupe de travail insiste sur la nécessité d'un « consentement spécifique » devant se rapporter à une situation « concrète et bien définie » et permettant de connaitre la finalité et le contexte dans lequel les données seront traitées[551].

Concrètement, les articles 10 et 11 de la Directive Européenne imposent une claire distinction entre l'information et le consentement. L'expression du consentement fondée sur le système du « double clic[552] » pourrait être une alternative de choix qui permettrait d'assurer l'expression d'un consentement non équivoque lors du traitement des différentes données recueillies. L'expression de la volonté de la personne doit donc passer par une information claire et accessible. Le traitement des données fondé sur le système du « double clic » peut se poser ainsi en deux étapes successives : tout d'abord, le responsable du traitement présenterait un formulaire indiquant à l'utilisateur la nécessité de recueillir les données en précisant leur nature (personnelle, médicale, fonctionnelle[553] etc.), il solliciterait ainsi une action de l'utilisateur qui devrait « cocher » une case pour chaque

[550] CNIL, Cookies et Traceurs : que dit la loi ? , www.cnil.fr
[551] Groupe de travail « l'article 29 » document WP131 sur les DME, 15 février 2007.
[552] Loi du 13 mars 2000 relative à la signature électronique, Insérée aux articles 1316 et suivants, cette loi prescrit que la signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant l'intégrité de l'acte.
[553] C'est-à-dire nécessaire au fonctionnement du site.

information faisant l'objet du traitement, conformément à nouvelle norme simplifiée n°48[554]. Cette première étape validée par la personne concernée permettrait d'accéder à un deuxième formulaire d'information précisant quels types de données pourraient faire l'objet de services associés ou de transfert vers des tiers. Dans le cadre d'un transfert à un tiers d'informations, le responsable destinataire du traitement devrait être soumis, à son tour, à une obligation d'information vis-à-vis de la personne concernée par le traitement. Une fois cette deuxième étape validée on considèrera que l'utilisateur a exprimé un consentement réel car il aura été informé des différentes utilisations des données qu'il consent à soumettre au traitement[555]. Cette information en deux étapes peut être rapprochée de l'obligation d'information renforcée du commerçant vis-à-vis du consommateur[556]. Dans le domaine de la santé, cette obligation d'information renforcée peut se rapprocher de l'obligation faite au médecin d'informer le patient sur l'intervention ou le traitement dont il va bénéficier, comme en dispose l'article L.1110-4 du Code de la santé publique.

Le nouveau dispositif de modernisation de notre système de santé 2016[557] intègre de nouvelles dispositions permettant une information plus efficiente du titulaire du dossier médical électronique[558]. En effet, l'article L.1111-21 du Code la santé publique dispose qu'un décret en Conseil d'Etat, pris après l'avis de la CNIL, devra énoncer les conditions de recueil du consentement et les conditions d'information auxquelles le titulaire devra avoir accès et qu'il pourra maîtriser. La création du dossier médical par les autorités, via internet, devrait permettre d'assurer la maîtrise des informations, notamment en assurant la neutralité des moyens de traitement des données. Le décret devrait prévoir « la nature et le contenu des informations contenues dans le dossier, les modalités d'exercice des droits des titulaires sur les informations figurant dans leur dossier »[559]. Cette clarté dans le contrôle des informations nécessite la même rigueur avec les prestataires de services. En particulier avec l'apparition des NTIC dans le domaine de la santé qui sont reliées à des plateformes sur l'internet qui ne relèvent pas d'un régime réglementaire propre à l'exercice d'une profession médicale.

---

[554] Norme simplifiée n°48 de la CNIL op.cit.loci.
[555] Le principe de loyauté issu de la directive impose aussi que la personne concernée soit également informé des conséquences d'un refus du traitement.
[556] Conformément à l'article 6 de Loi n° 2014-344 du 17 mars 2014 relative à la consommation, dite Loi Hamon.
[557] Projet de loi de modernisation de notre système de santé (AFSX1418355L)
[558] Nouvellement renommé en dossier médical partagé.
[559] Article 25 du projet de modernisation de notre système de santé modifié le 15 avril 2015.

168. ***Conclusion.-*** Il est désormais primordial que les autorités mettent en place un dialogue avec les différents prestataires sur le marché de la santé afin de définir un cadre légal strict, notamment avec la mise en place de l'open data. Ce dernier représente une base d'informations gérée par la sphère publique. Il permettrait d'éviter la dispersion des données générées par chaque individu, car la loi ne peut pas gérer la protection et l'édition de données par la personne elle-même. Cette possibilité de divulgation, mais aussi de protection, passe par des applications techniques[560] au sein des logiciels dits « privacy by design » (confidentialité dès la conception) permettant de gérer l'utilisation de données personnelles et de ne pas être traqué par des enseignes commerciales avec, par exemple, l'ajout par Microsoft à son Internet Explorer du « do not track by default [561]», ce que l'on appelle le « privacy by default ». On peut également citer la limitation de conservation à six mois des données de connexion d'une adresse IP comme une bonne pratique[562].

Enfin, le Conseil Economique Social et Environnemental préconise la généralisation de tableaux de bord (dashboard) qui permettent à l'internaute d'avoir accès, à tout moment, à une page sécurisée relevant l'ensemble des données récoltées sur lui, celles nécessaires dans le service qui lui est rendu ainsi que celles que l'opérateur s'apprête à délivrer à un tiers. Sur ces différents points, et, tout particulièrement sur le dernier, la personne doit pouvoir exercer son consentement, afin d'autoriser ou pas la communication de ses informations à un tiers.

[560] Une solution avancée par l'ASIP Santé est de généraliser le recours à un identifiant national de santé (INS). Une obligation légale pourrait obliger un prestataire proposant un service à caractère médical, d'en définir la finalité afin qu'il intègre un système d'interopérabilité avec les autorités publiques telles que la CNIL ou la HAS.
[561] Qui permet de ne pas déposer des cookies sur la machine de l'utilisateur de façon systématique.
[562] Cahier IP, op.cit.loci. Page 15

Chapitre 3 : Le régime spécifique de la protection des données de santé à caractère personnel

Le traitement des données de santé à caractère personnel implique, dans un premier temps, l'étude de la protection spécifique relative aux informations de santé (section 1) afin d'effectuer une analyse de la protection informatique du secret médical (section 2). Cette analyse permet d'envisager les nouveaux paramètres qu'implique l'ouverture du marché des données de santé à caractère personnel à des acteurs qui ne sont pas soumis au régime spécifique des professionnels de santé (Section 3).

Section 1 : Le secret médical et les données de santé

169. Le secret médical.- Ce principe figure à l'article 4 du Code de déontologie médicale. Selon ce texte, « le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris ». L'article 73 ajoute que « le médecin doit protéger contre toute indiscrétion les documents médicaux concernant les personnes qu'il a soignées ou examinées, quels que soient le contenu et le support de ces documents. Il en va de même des informations médicales dont il peut être le détenteur ». La règle figure également dans plusieurs autres textes de droit positif[563]et est présentée par le Comité Consultatif National d'Ethique[564] comme « un principe essentiel à l'édification d'une relation confiante entre les médecins et les patients ». Plus largement, elle est intégrée dans le principe du secret professionnel[565] et c'est à ce titre que le droit pénal en réprime la violation. En effet, « la révélation d'une information à caractère secret

[563] Code de la santé publique, art. L. 1112-1 et art. L. 4314-3; point 8 de la Charte du patient hospitalisé du 6 mai 1995 et est présentée par le Comité consultatif national d'éthique (avis n° 76 du 24 avril 2003).
[564] Comité consultatif national d'éthique, avis n° 76 du 24 avril 2003.
[565] Art. 26 de la loi n° 83-634 du 13 juillet 1983 portant statut général des fonctionnaires

par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 € d'amende »[566]. Il faut noter, par ailleurs, que la règle du secret médical est associée à celle du respect dû à la vie privée qui est posée tant par le droit interne que par le droit international[567]. Le code civil qui peut ici être invoqué affirme que « chacun a droit au respect de sa vie privée ».

170. Les personnes tenues au secret médical.- La formulation de l'article 226-13 du Code pénal est large. Elle établit une véritable « chaîne du secret ». Au-delà des médecins, le silence s'impose à tous ceux qui concourent directement ou indirectement à la délivrance des soins[568]. Les personnels administratifs y sont astreints comme les autres. La règle concerne donc les agents et responsables des services d'assurance maladie. A fortiori, elle s'applique normalement aux membres des équipes de recherche pour la part d'informations qu'ils détiennent.

171. Les exceptions classiques au principe du secret médical.- Il existe des hypothèses dans lesquelles un professionnel de santé est autorisé à révéler une information confidentielle. Ce sera le cas chaque fois que l'intérêt de la société doit prévaloir sur celui de l'individu. Ces dérogations sont toutefois énumérées de manière limitative par les textes[569]. Elles sont obligatoires, dès lors qu'il s'agit de protéger la santé publique, mais seulement dans les hypothèses de risques épidémiologiques ou contagieux[570]. Il en va de même lorsqu'il importe de préserver l'intérêt du patient, mais il ne s'agit que d'hypothèses où il existe une menace, une affection ou un dommage déjà réalisé pour des individus donnés. Le code de la sécurité sociale prévoit une communication obligatoire par les praticiens du code des actes effectués, des prestations servies aux assurés et des pathologies diagnostiquées aux organismes d'assurance maladie dans le but de maîtriser les dépenses de santé[571].

---

[566] Art. 226-13 du code pénal
[567] Art. 10 de la Déclaration Universelle des Droits de l'Homme du 10 décembre 1948 ; art. 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950.
[568] CE 11 février 1972, Crochette, recueil Lebon, p. 138
[569] CE 31 mai 1989, Mme Roujansky, Lebon, p. 135
[570] Art. L. 3113-1 CSP ; décret n° 99-363 du 6 mai 1999 fixant la liste des maladies faisant l'objet d'une transmission obligatoire de données individuelles à l'autorité sanitaire et modifiant le code de la santé publique.
[571] Art. L. 161-29 Code de la sécurité sociale.

172. La protection spécifique des données nominatives informatisées dans le domaine médical.- Depuis 1994, la protection des données nominatives à caractère médical est organisée expressément par le droit. La loi du 1er juillet 1994 a, d'abord, consacré l'idée que les informations « ayant pour fin la recherche dans le domaine de la santé » devaient faire partie des données nominatives considérées comme sensibles. La constitution de fichiers est, depuis lors, subordonnée à une autorisation de la CNIL, après avis d'un comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé. Le 24 octobre 1995, la directive européenne a incité les Etats membres de l'Union européenne à inclure plus largement les « données relatives à la santé » dans la liste des informations nominatives faisant l'objet d'une interdiction de traitement informatisé[572]. Ce ne sont donc plus seulement les données destinées à la recherche qui sont visées, mais toutes les données à caractère médical.

173. La collecte des données nominatives informatisées par la CNAM.- En principe, les tiers ne sont pas autorisés à avoir accès aux données nominatives à caractère médical. La notion de tiers recouvre toute personne autre que le médecin, notamment son secrétariat et la personne examinée par le praticien[573]. Néanmoins, cette exclusion des tiers ne fait pas obstacle à l'existence d'un traitement informatisé des données recueillies par la CNAM auprès des médecins et cela aux fins de gestion du système de l'assurance maladie[574]. Cependant, le Conseil Constitutionnel[575] a insisté sur la nécessité d'« une particulière vigilance dans la transmission des informations nominatives à caractère médical entre les médecins prescripteurs et les organismes de sécurité sociale ». Il insiste également sur la nécessité de mettre en place des modalités d'acheminement des documents nominatifs qui permettent d'assurer « la stricte confidentialité de la transmission des informations qu'ils contiennent ». Le juge administratif estime, quant à lui, que la transmission des données à des « organismes concentrateurs techniques » chargés d'acheminer ces informations vers les organismes de sécurité sociale répond à l'exigence de confidentialité dès lors que les données sont communiquées, « pour l'essentiel, sous une

[572] Art. 8, § 1 de la directive 95/46/CE du 24 octobre 1995 op. cit. loci.
[573] Cass. crim. 30 octobre 2001, n° 99-82136, inédit.
[574] Art. L. 161-29 al. 2, Code de la sécurité sociale, art. L. 161-29 al. 2.
[575] Conseil Constitutionnel, 21 décembre 1999, Dec. n° 99-422, Loi de financement de la sécurité sociale pour 2000, Rec. p. 143 ; AJDA 2000, p. 48, note J.-E. Schoettl.

forme codée » et que « ces organismes agissent sous l'autorité des médecins »[576]. Il reste à savoir dans quelle mesure la maîtrise des dépenses de santé est susceptible d'autoriser une communication des données nominatives aux organismes d'assurance maladie et vers les équipes de recherche pharmacologique.

174. Les dérogations légales à la confidentialité des données à caractère médical.- Au-delà des apparences, le secret médical se trouve, en réalité, dans une situation paradoxale. Alors que son principe a fait incontestablement l'objet d'une protection accrue dans le domaine informatique depuis l'apparition et le développement des Nouvelles Technologie de Communication et de l'Information (NTIC), il apparaît qu'au nom des impératifs de la santé publique, son aménagement juridique pourrait connaitre une évolution.

175. La valeur constitutionnelle du principe de protection de la santé.- La protection de la santé figure à l'article 25 de la Déclaration universelle des droits de l'Homme du 10 décembre 1948, à l'alinéa 11 du préambule de la Constitution du 27 octobre 1946 ainsi que dans un certain nombre d'autres textes européens et internationaux. Ce principe fait l'objet d'une protection par le Conseil constitutionnel[577]. En effet, il s'agit d'un principe ou objectif à valeur constitutionnelle, ce qui étend considérablement sa portée. En effet, il est « admis que la notion d'objectif à valeur constitutionnelle permet au juge de justifier fonctionnellement l'atteinte à certains droits fondamentaux par une loi poursuivant l'intérêt général [578]». Ce but est donc de nature à justifier une restriction au principe du respect de la vie privée, « car la santé au sens constitutionnel revêt une dimension prioritairement collective [579]». Cela se traduit par le contrôle du juge pour définir la *santé publique* comme une fin « d'intérêt général »[580]. Cette dimension collective

[576] CE 13 novembre 2002, Conseil national de l'ordre des médecins, req. n° 234087 ; voir aussi, art. L. 161-34 du code de la sécurité sociale.
[577]15 janvier 1975, n° 74-54 DC, Interruption volontaire de grossesse, Rec. p. 19 ; Les Grandes Décisions du Conseil constitutionnel, Dalloz, n° 23 ; cf. J. Moreau, Le droit à la santé, AJDA 1998, p. 186 ; J. Moreau, D. Truchet, Droit de la santé publique, Dalloz, 1995 ; J.-M. de Forges, Le droit de la santé, PUF, 1997.
[578] B. Faure, Les objectifs de valeur constitutionnelle, Rev. fr. dr. const. 1995, p. 47 et s.
[579] Ibidem.
[580] V. Saint-James, Le droit à la santé dans la jurisprudence du Conseil constitutionnel, RD publ. 1997, p. 460 ; L. Casaux-Labrunée, Le droit à la santé, *in* R. Cabrillac, M.-A. Frison-Roche, T. Revet, Libertés et droits fondamentaux, Dalloz, 2003, p. 698.

autorise alors des restrictions aux libertés individuelles parmi lesquelles figure le secret médical.

176. La primauté de la maîtrise des dépenses de santé.- D'après le Conseil constitutionnel, la reconnaissance de la « protection de la santé publique » va de pair avec la « maîtrise de l'évolution des dépenses de santé », les deux notions se conditionnant mutuellement[581]. Dès lors, la volonté « de remédier à l'augmentation excessive [de ces] dépenses et à leur caractère éventuellement injustifié » est un motif légitime pour autoriser la transmission à des tiers des données nominatives à caractère médical[582]. On ne saurait y voir a priori une atteinte au respect de la vie privée. Tout en rappelant que le mécanisme d'autorisation par la CNIL s'avère nécessaire pour la protection individuelle, le Conseil constitutionnel ne semble pas s'opposer à un aménagement du secret professionnel si deux conditions sont respectées. Dans un premier temps, toute communication de données doit être fondée en droit. Dans un second temps, cette communication doit respecter la confidentialité des informations délivrées[583]. Le législateur doit donc « concilier le droit au respect de la vie privée et l'exigence de valeur constitutionnelle qui s'attache à l'équilibre financier de la sécurité sociale »[584].

La possibilité de transmettre à des tiers des données nominatives à caractère médical a ainsi été adoptée par la loi n° 2016-41 du 26 janvier 2016 « de modernisation de notre système de santé ». Ce texte renforce le cadre juridique permettant que soient menées de manière indépendante de l'administration des analyses ou des évaluations du système de santé, dont les conditions sont visées à l'article 53 de la « LIL » modifiée. Désormais, le traitement de données personnelles en provenance de dossiers médicaux détenus aussi bien par les médecins libéraux que dans les systèmes d'information des caisses d'assurance maladie, est autorisé dans le but d'évaluer les pratiques de soins et de prévention. La communication de ces données ne peut se faire que sous la forme de « jeux de données agrégées ou des échantillons, issus des traitements des données de santé à caractère personnel pour des finalités et dans des conditions reconnues conformes à la présente loi

[581] Cons. const. 21 décembre. 1999, n° 99-422, op.cit.loci.
[582] Ibidem.
[583] Cons. const. 23 juillet 1999, n° 99-416 DC, loi portant création d'une couverture maladie universelle, Rec. p. 100 ; AJDA 1999, p. 700, note J.-E. Schoettl.
[584] Cons. const. 21 décembre 1999, n° 99-422, op.cit.loci.

par la Commission nationale de l'Informatique et des Libertés, [585]» de sorte à ce que la personne concernée ne puisse pas être identifiée.

177. Les conditions de réalisation d'une enquête de santé publique.- Selon la loi n°2016-41 du 26 janvier 2016, chaque demande de communication aux fins de constitution d'un fichier fait l'objet d'une autorisation de la CNIL qui vérifie les garanties présentées par le demandeur et l'opportunité du projet. Elle fixe « la durée de conservation des données nécessaires au traitement et apprécie les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi » conformément à l'article 27 de la loi de 1978 modifiée par la loi n°2016-41 du 26 janvier 2016[586].

La qualification juridique de la phase préliminaire de l'enquête.- Il s'agit de savoir si la phase préliminaire d'une enquête doit être considérée ou non comme un « traitement de données à caractère personnel[587] ». La directive européenne encadre « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction »[588]. Il n'est pas certain que l'on puisse qualifier cette situation de « traitement de données à caractère personnel » car il y a eu « collecte » suivie de « communication par transmission », le tout par voie informatique[589]. Si, comme on peut le penser, la phase

[585] Art 54, V de la loi « Informatique et Libertés » modifiée.
[586] Dans l'affaire Cadeus, la CNIL a exercé son contrôle et rendu un avis favorable le 19 mai 2003. En effet, si le département de pharmacologie de l'université de Bordeaux a reçu l'autorisation d'utiliser la base de données de la Sécurité sociale, c'est parce que l'enquête a été jugée conforme aux exigences de confidentialité prescrites : la CNAM tire au sort au début de chaque mois les dossiers informatisés qui seront délivrés ; elle les transmet aux responsables de l'enquête par fourgon blindé ; les dossiers sont communiqués sur un CD-Rom crypté deux fois qui ne peut pas être copié sur un ordinateur et qui est stocké dans un coffre-fort. Par ailleurs, les membres de l'équipe ont signé un engagement de confidentialité et sont soumis au secret professionnel conformément à la loi de 1978. Les résultats de l'étude seront purement statistiques et ne permettront en aucune manière l'identification, même indirecte, des personnes concernées. Enfin, l'enquête est limitée dans le temps, puisque le protocole prévoit qu'elle se déroulera de septembre 2003 à septembre 2004. A son terme, l'ensemble des informations à caractère nominatif seront détruites. Sur ces divers points, l'enquête de santé publique présente d'indéniables garanties.
[587] Art. 2-b de la directive 95/46/CE.
[588] Ibidem.
[589] CE Ass. 30 juin 2000, Ligue française pour la défense des droits de l'Homme, AJDA, 2000, p. 831, concl. P. Fombeur.

préliminaire de l'enquête répond aux critères d'un traitement informatisé de données nominatives à caractère personnel et n'en est pas détachable, il faut alors émettre de sérieuses réserves sur les conditions dans lesquelles la confidentialité de ces données a pu être garantie.

178. La matière couverte par le principe de confidentialité.- Selon l'article 8 la loi de 1978, modifiée par la loi du 6 août 2004, les données personnelles dont le traitement est envisagé ne doivent comporter « ni le nom, ni le prénom des personnes concernées, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques ». De plus, les traitements autorisés « ne peuvent servir à des fins de recherche ou d'identification des personnes ». Or, « le traitement des dossiers communiqués par la CNAM, même s'il a pour finalité la réalisation d'une analyse statistique, n'en comporte pas moins un but intermédiaire qui est la recherche des personnes concernées afin d'obtenir leur consentement et même leur participation (en cas de refus de la personnes contactée, toute donnée la concernant est supprimée du fichier). Cette recherche ne peut évidemment se faire qu'au prix de la divulgation du nom et des coordonnées des patients. Il est donc légitime de se demander s'il n'y a pas eu violation de la loi.[590] ». La jurisprudence considère généralement que des données deviennent confidentielles dès lors qu'elles sont susceptibles de révéler le type d'affection dont le malade est atteint. Le juge judiciaire et le juge administratif estiment ainsi que le simple fait de communiquer à un tiers l'existence et le nom d'un malade pour permettre à ce tiers d'entrer en contact avec lui est une violation du secret médical, même s'il n'y a pas eu de révélations médicales à proprement parler[591].

---

[590] Ph. Ségur, « *Confidentialité des données médicales, A propos des enquêtes de santé* », AJDA 2004 p.858. Voir aussi, D. Houssin, « *Le secret médical dans les nouvelles pratiques et les nouveaux champs de la médecine »,* Recueil Dalloz 2009*,* p 2619.

[591] CE 1er juin 1994, CHS Le Valmont, Gaz. Pal. 14-16 juillet 1996, p. 97 Document InterRevues ; dans le même sens, Cass. 1re civ. 24 février 1993, Bull. civ. I n° 87. Dans cette affaire, les intéressés ont soutenu que l'identité des personnes n'était utilisée que pour envoyer les courriers préalables aux patients et aux médecins. Ce n'est qu'avec leur consentement que les enquêteurs pourront ensuite accéder aux données de soins les concernant. Dès cet instant, le programme informatique associera aux informations médicales un « identifiant », différent du numéro de Sécurité sociale, qui ne permettra plus aux chercheurs de connaître les noms des patients ou de leurs médecins. Cette garantie, bien que sérieuse, ne lève pas l'objection. En effet, au stade de l'envoi du courrier préalable, l'utilisation des données n'est ni neutre ni indifférenciée, puisqu'elle est réalisée à partir d'une sélection opérée par la CNAM sur un critère médical prédéfini : la prescription d'AINS. A partir des listes communiquées, on déduit donc nécessairement les traitements suivis par les destinataires des courriers ainsi que les affections probables dont ils sont atteints.

Le nouveau cadre juridique mis en place par la nouvelle loi de modernisation de notre système de santé[592] permet de garantir la confidentialité des données, notamment grâce à la mise en place des Référentiels Généraux de Sécurité (RGS). Ces référentiels permettent le partage d'informations entre les différents maillons de la prise en charge du patient tout en préservant « le droit au respect de la vie privée du malade et le secret des informations le concernant ».

Le traitement des données à caractère médical s'effectue par différentes techniques, notamment grâce au Système d'Information (SI)[593]. Comme envisagé précédemment, les informations à caractère médical sont tout d'abord amenées à « passer de main en main ». Ce n'est qu'après un traitement par le personnel médical que ces informations seront [télé]transmises via un réseau immatériel ou électronique.

179. L'interopérabilité des services.- C'est la finalité de la loi du 13 août 2004 relative à l'assurance maladie[594] ainsi que de la loi du 22 juillet 2009 Hôpital Patient Santé Territoire (HPST)[595]. Cette volonté du législateur vise une action coordonnée des acteurs, laquelle constitue la clé de voute d'une prise en charge efficiente du patient. Cette loi ambitionne également une réduction des coûts de santé publique.

Cette interopérabilité doit se faire au travers d'un système de traitement des données afin que les informations qui en sont extraites puissent être utiles au parcours de soins du patient. Elle devrait aussi faciliter l'ouverture des droits au remboursement. C'est également l'objectif affiché de la loi du 26 janvier 2016 de modernisation de notre système de santé[596].

---

[592] Loi du 26 janvier 2016 op. cit. loci.

[593] « *Le système d'information est l'ensemble des informations formalisables circulant dans l'entreprise et caractérisées par des liens de dépendance, ainsi que des procédures et des moyens nécessaires pour les définir, les rechercher, les formaliser, les conserver, les distribuer*. » Système d'information (Gestion de l'information) par A.Semoud et A.Laymy, mémoire en informatique et communication, Université Hassan II Mohammedia, 2006.
« Le SI doit être considéré […] comme une base jeune. Les limites actuelles doivent donc être appréciées relativement aux progrès déjà accomplis, mais surtout au regard des études que l'on entend réaliser. Les besoins en données dépendent des usages. » *Rapport sur la gouvernance et l'utilisation des données de santé*, Pierre – Louis Bras, inspecteur général des affaires sociales. Page 21.

[594] Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie.

[595] Article 51 de la Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, ajoutant un livre préliminaire relatif à la coopération entre professionnel de santé.

[596] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JORF n°0022.

180. L'article 9 de l'ordonnance n°2005-1516 du 8 décembre 2005[597] a créé les Référentiels Généraux de Sécurité (RGS)[598] afin de parvenir à une coordination des moyens de communiquer par voie électronique. Dans le cadre de cette étude, les RGS sont déclinés avec le Référentiel Général d'Interopérabilité (RGI) disposé à l'article L.1111-8 alinéa 4[599] du Code de la santé publique. Cet article régit les échanges électroniques entre les usagers et les autorités administratives. Ces échanges doivent permettre un transfert sécurisé des informations de santé.

L'enjeu de l'interopérabilité est de rendre la communication compréhensible au travers d'un ensemble de conventions techniques que l'on peut qualifier de « système formel ».

En pratique, les conventions d'interopérabilité conduisent à des protocoles que chaque concepteur doit respecter. Les éditeurs de produits de sécurité et les prestataires de services de confiance sont également visés par ces conventions, dans la mesure où ils doivent proposer aux autorités administratives des produits et des prestations conformes aux exigences du RGS.

La Commission Européenne, dans sa recommandation du 2 juillet 2008, a défini l'interopérabilité des systèmes des dossiers de santé comme « la capacité de plusieurs systèmes de dossiers informatisés de santé d'échanger aussi bien des données exploitables par un ordinateur que des informations et des connaissances demandant une intervention humaine [600]».

181. Les référentiels d'interopérabilité et de sécurité sont visés par l'alinéa 4 de l'article L.1111-8[601] du Code de la santé publique qui définit les mesures de sécurisation

---

[597] Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives (ratifiée par l'article 1398 I de la loi n°2009-526 du 12 mai 2009), J.O.R.F du 9 décembre 2005.

[598] Le RGS traite des fonctions de sécurité permettant l'authentification, signature électronique, chiffrement, horodatage. Disponible sur http://www.ssi.gouv.fr.

[599] La détention et le traitement sur des supports informatiques de données de santé à caractère personnel par des professionnels de santé, des établissements de santé ou des hébergeurs de données de santé à caractère personnel sont subordonnés à l'utilisation de systèmes d'information conformes aux prescriptions adoptées en application de l'article L. 1110-4 et aux référentiels d'interopérabilité et de sécurité arrêtés par le ministre chargé de la santé après avis du groupement mentionné à l'article L. 1111-24.

[600] Recommandation n°2008/594/CE de la Commission Européenne du 2 juillet 2008 sur l'interopérabilité transfrontalière des dossiers informatisé (263).

[601] Ordonnance n° 2010-177 du 23 février 2010 de coordination avec la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

physique et logique, les modalités d'accès, les modalités de traitement, les mesures d'identification, les mesures d'habilitation, les procédures de traçabilité, les historiques concernant les accès aux informations et les mesures mises en œuvre pour garantir la confidentialité dont le chiffrement de tout ou partie des informations recueillies[602].

La première version du RGI a été diffusée le 12 juin 2009 par la Direction Générale de la Modernisation de l'Etat (DGME) et approuvée par arrêté du 11 novembre 2009[603]. Le cadre « d'interopérabilité des systèmes d'information en santé » a été soumis à la concertation de l'ASIP Santé en septembre 2009. Le 25 février 2010, l'ASIP Santé a publié la nouvelle version du document en vue d'une mise en place effective au cours du troisième trimestre 2010. L'Agence indique que les objectifs de gouvernance devront être basés sur « une sélection de normes et standards adaptés au contexte des [systèmes d'information] de santé français », ces objectifs devront prendre en compte également « la réalité opérationnelle du terrain » en collaboration avec « les stratégies des industriels français et européens » dans le but de garantir leur développement industriel avec stabilité.

L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) en collaboration avec la Direction des Grandes Entreprises (DGE), ont quant à elles, rédigé les référentiels généraux de sécurité qui ont été approuvés et mis en ligne le 18 mai 2010 et publiés le même jour au journal officiel avec l'arrêté approuvant le référentiel[604]. La dernière version des RGS prise par arrêté en date du 14 juin 2014[605] dispose que les référentiels se composent d'une certification électronique, d'un horodatage et d'audit de la sécurité des systèmes d'information. Cette dernière version dites « 2.0 » abroge donc la mise en place prévue par l'arrêté du 6 mai 2010 dans ses modalités de mise en œuvre des référentiels et dispose que « les autorités administratives ne sont tenues d'accepter les certificats électroniques et les contremarques de temps conformes aux annexes du référentiel général de sécurité approuvé par le présent arrêté [du 13 juin 2014] qu'à compter du 1er juillet 2015. ».

---

[602] Art. R. 1110-1 CSP.
[603] Document disponible sur http://www.references.modernisation.gouv.fr/.
[604] Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, J.O.R.F 18 mai 2010.
[605] Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, JORF n°0144 du 24 juin 2014.

Dans le même sens, le décret dit « décret confidentialité » n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le Code de la santé publique reprend dans ses dispositions la mise en place des référentiels en indiquant que les référentiels régissent notamment :

« Les mesures de sécurisation physique des matériels et des locaux ainsi que les dispositions prises pour la sauvegarde des fichiers ; les modalités d'accès aux traitements, dont les mesures d'identification et de vérification de la qualité des utilisateurs, et de recours à des dispositifs d'accès sécurisés ; les dispositifs de contrôle des identifications et habilitations et les procédures de traçabilité des accès aux informations médicales, ainsi que l'histoire des connexions ; en cas de transmission par voie électronique entre professionnels, les mesures mises en œuvre pour garantir la confidentialité des informations échangées, le cas échéant, par le recours à un chiffrement en tout ou partie de ces informations.[606] »

182. Le « décret confidentialité » dispose également de la mise en œuvre de l'utilisation de matériels permettant d'accéder aux informations mais permettant aussi la production d'informations qui alimentent les bases de données. Le Code de la santé publique dispose d'une obligation pour les professionnels de santé ou les établissements d'utiliser une carte professionnelle de santé[607]. Cette carte est issue du « décret confidentialité » et est utilisée « en cas d'accès par des professionnels de santé aux informations médicales à caractère personnel conservées sur support informatique ou de leur transmission par voie électronique [608]». L'accès aux données de santé hébergées est donc subordonné à l'utilisation de la carte professionnelle de santé qu'elles figurent ou non dans le dossier de santé. La CPS est donc un instrument qui permet de « tracer » son titulaire lorsqu'il accède aux données de santé du patient. La carte professionnelle de santé est mentionnée à l'article L.161-33 du Code de la sécurité sociale et est une réelle garantie

[606] Art. R. 1110-1 du Code de la santé publique.
[607] Art. R. 1110-3 En cas d'accès par des professionnels de santé aux informations médicales à caractère personnel conservées sur support informatique ou de leur transmission par voie électronique, l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du Code de la sécurité sociale est obligatoire ».
[608] Art. 1110-3 du Code de la santé publique.

de protection pour le patient puisque le professionnel devra s'authentifier pour accéder aux informations médicales le concernant.

Il semble que le niveau de sécurité prévu par le législateur soit propice au renforcement des garanties protégeant le secret des informations médicales en matière d'échanges informatiques. Cependant, il semble que le secret médical ne soit pas toujours garanti compte tenu de la diversité des données pouvant contenir des informations médicales.

Section 2 : L'évolution du cadre juridique et le Big Data

183. De l'art médical au commerce.- La directive commerce électronique du 8 juin 2000[609] définit de manière large le prestataire d'un service de la société de l'information et assimile incontestablement le médecin qui offre des services de télémédecine à l'ensemble des autres prestataires, qu'il s'agisse de publicité, d'informations préalables ou de règles à suivre dans le processus contractuels. Cette application de la directive[610] sur la libre prestation de services connue sous le nom de la directive Bolkestein au sein des professions libérales[611], a pour conséquence d'ouvrir l'ensemble du territoire européen à la concurrence entre prestataires de soins de santé[612].

Cette ouverture des marchés et cette assimilation de celui qui pratique un art, jusqu'ici libéral, à un marchand introduisent une logique économique dans le secteur des soins de santé. Cette considération contribue très certainement à ce que le patient considère « La » relation avec « son » médecin comme une transaction qui doit être appréciée comme toute autre transaction au terme d'un « forum shopping [613]». Les services sur le web ou via le web vont-ils remplacer pour partie le professionnel de santé dès lors que le patient pourra s'informer davantage sur internet des caractéristiques de sa maladie, de certains

[609] Sur l'application de la directive e-commerce 2000/1/CE du 8 juin 2000 aux services de santé, lire P. van Eecke, « Electronic Health record Services and the e-commerce directive », in *A decade ofresearch the crossroad of law and ICT,* J. Dumortier et F. Robben édition Larcier, 2001.
[610] H.Herveg, « Panorama des responsabilités liées aux services et produits de santé en ligne en droit européen », *RDTI,* 2008, n°68 et s.
[611] Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur.
[612] S. Francq et O. De Schutter, « la proposition de directive relative aux services dans le marché intérieur : reconnaissance mutuelle, harmonisation et conflits de la loi dans l'Europe en ligne », *Cahiers de droit européen,* 2005, p.604 et s.
[613] Conseil de l'ordre des Médecins sur les dangers des prescriptions par voie électronique, *Avis du Conseil du* 19 août 2000, B.O, n°90, p.13.

médicaments ou des risques liés au traitement proposé ? Dans la même façon, le test d'auto-diagnostic sur l'internet et tels qu'envisagés dans la directive 98/79 à propos des dispositifs de diagnostic in vitro constituent déjà une transformation de la notion de « patient » en « consommateur[614] ».

184. Le cas du « surcodage » effectué par des tiers opérateurs.- Les départements d'information médicale sont devenus des services déterminants dans le système de financement des établissements de santé. Ce que n'ont pas manqué d'observer des sociétés privées, spécialisées dans le codage des données médicales, qui se sont lancées sur le marché. La mission de ces entreprises est de vérifier si des actes n'ont pas été oubliés et d'envoyer la nouvelle facture à la Sécurité Sociale. « On fait du contrôle qualité. On traque les oublis », résume T. Dispot, responsable de Medlink[615]. Si celles-ci ont obtenu auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) une autorisation pour consulter les résumés de séjour des patients, anonymes, dans les faits, elles accèdent aux dossiers médicaux. « Nous consultons des fichiers anonymes, mais dans la pratique on va voir dans les dossiers médicaux des patients. C'est la seule méthode pour optimiser le codage », reconnaît Thierry Dispot. Et c'est là que le bât blesse. D'après le Code de santé publique, les données médicales des patients ne peuvent pas être consultées par des sociétés externes à l'hôpital. Ce sont justement les arguments avancés par le Docteur Tanquerel à sa direction pour refuser que l'entreprise Altao[616] intervienne sur l'hôpital de Saint-Malo. « La CNIL les autorise à accéder à des résumés de sorties anonymes, mais ceux-ci sont indirectement nominatifs dans la mesure où ils comportent la date de naissance du patient, sa date d'entrée et sa date de sortie. En outre, ils accèdent aux fichiers des patients. Qui nous dit qu'ils ne se constituent pas une base de données », incrimine le praticien, qui martèle : « Le médecin DIM est le garant du secret médical, le seul médecin de l'hôpital à avoir accès à tous les dossiers médicaux. Si j'avais permis à cette société de

[614] N. Fraselle, « *Du patient au consommateur, la construction d'un combat social »,* Louvain la Neuve, Academia-Bruylant, 2000, 226p.

[615] *Medlink Ports* développe une gamme de services à valeur ajoutée innovants pour ses clients : chargeurs, transitaires, transporteurs. Ces services, dont certains sont en cours de développement ont notamment pour objectifs proposer un Dossier Médical numérique.

[616] La société *Altao* participe à l'amélioration de la santé de ses concitoyens en aidant les établissements de soins à améliorer leur stratégie, leur organisation et leur gestion. Altao met à disposition de ses clients une équipe pluridisciplinaire (médecins, ingénieurs, statisticiens, gestionnaires) qui unit l'ensemble de ses compétences pour accompagner les établissements de santé de la manière la plus efficace qui soit. *Qui sommes nous ?, www.altao.com.*

les consulter, je me serais rendu coupable d'un délit. » Des arguments balayés par le responsable de Medlink : « nous travaillons en collaboration avec le médecin DIM et l'accord de la commission médicale d'établissement (CME). Si le médecin n'est pas d'accord, on n'intervient pas », explique Th. Dispot.

Depuis deux ans, les dossiers médicaux des patients contenant diagnostics et prises en charge, et qui permettent aux établissements de santé de se voir attribuer les moyens financiers à hauteur de leur activité, continuent dans certains établissements à se voir confiés à des sociétés privées ne garantissant pas la confidentialité des données, ni le respect du secret médical.

Depuis deux ans, les médecins des départements d'informatique médicale « DIM », experts du codage mais aussi garants de la déontologie, continuent à subir des pressions très fortes de la part des établissements qui les obligent à fournir à ces sociétés privées des données non anonymisées, ne respectant pas le secret médical. D'autant que ces sociétés privées sont rémunérées au prorata du surcodage qu'elles pratiquent, surcodage effectué, bien sûr, au détriment de l'Assurance Maladie.

L'exemple du surcodage informatique permet de mettre en relief l'enjeu que représentent les données traitées au cours d'un diagnostic ou non. Il s'agit, en l'espèce, de faire une corrélation avec la décision du Conseil d'Etat du 15 décembre 2010 qui indique que le secret médical couvre les informations qui sont issues d'un diagnostic, mais, également les informations qui ne sont pas issues d'un diagnostic.

Par conséquent, il convient d'admettre la nécessité de reconnaître un régime particulier en ce qui concerne les informations de santé collectées hors diagnostic, afin de soumettre le maître du traitement au secret médical.

185. Les données de santé et les objets connectés.- Comme nous l'avons déjà envisagé précédemment, les données de santé peuvent prendre diverses formes. Il convient de mettre en relief que les données de santé *traditionnelles* et les données de santé issues des objets connectés sont soumises au même régime de protection que celui prévu pour les données à caractère personnel. Or, les données de santé ont le même caractère « sensible » quelle que soit leur provenance. De fait, il convient de s'en remettre à l'article 8 I de loi «Informatique et Libertés» qui impose l'interdiction de collecter des données faisant

apparaître de façon directe ou indirecte des données qui « sont relatives à la santé » de la personne concernée[617]. Comme exposé précédemment, ce principe connaît une exception, lorsque la personne concernée a exprimé son consentement, ou encore, lorsque ces données présentent une finalité nécessaire en matière de traitement ou à des fins de recherches[618]. Enfin, le §III de la loi «Informatique et Libertés» modifiée autorise l'utilisation des données lorsqu'elles font l'objet d'un bref procédé d'anonymisation.

Le champ de protection des données de santé recouvre ainsi toutes les données qu'elles soient issues du domaine médical traditionnel ou des objets connectés. Cela dit, compte tenu du volume de données traitées et collectées grâce aux objets connectés, on peut s'interroger sur la qualité du consentement de la personne qui consent à ce que ses données soient collectées et traitées via les objets connectés. C'est ce que remarque, non sans ironie, certains auteurs qui doutent précisément du caractère « éclairé » du consentement exprimé[619].

186. Des entreprises privées non soumises au régime juridique des professionnels de santé.- Les nouveaux opérateurs internet proposant des produits *Quantifed self* ne sont pas soumis aux règles prévues par le Code de santé publique. En effet, la procédure d'agrément concerne les hébergeurs de données de santé dans un certain cadre d'activité comme la prévention ou la continuité des soins, mais elle ne permet pas de tenir compte des nouvelles données générées directement par la personne et confiées à une entreprise privée. Mme Le Professeur Mendoza remarque que « dans un monde interconnecté, l'anonymat des données est-il encore possible ? Le risque de ré identification de la personne à partir de données anonymes est avéré[620] » et que l'évolution des technologies du Big Data rendent « la notion d'« *anonymat* » désormais illusoire et les procédés

[617] Article 8-I modifié de la loi n° 78-17 du 6 janvier 1978 : « *Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.* »

[618] Article 8 II, LIL op. cit .loci.

[619] A. Mendoza-Caminade, « *Big data* et données de santé : quelles régulations juridiques ? », Rev. Lamy droit de l'immatériel n°127, 2016, page4 ; S. Gambardella, Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé, RDSS 2016 p.271.

[620] A. Mendoza-Caminade, *Big data* et données de santé : quelles régulations juridiques ?, op cit loci

techniques d'anonymisation ne constituent plus des garanties[621]». Il convient d'ajouter que des nouveaux modes d'interconnexion sont à prendre en compte, notamment avec la possibilité laissée à l'utilisateur de se connecter à d'autres applications et de partager ses informations de santé avec d'autres prestataires ou utilisateurs.

Il serait difficile d'imposer le régime d'autorisation préalable en vigueur et il ne serait pas « pertinent[622] » d'imposer un régime propre d'autorisation aux dispositifs mobiles, mais, il serait envisageable de créer une distinction selon la provenance des données.

187. Le régime des dispositifs médicaux appliqué à la santé connectée.- Les dispositifs médicaux sont visés à l'article L5211-1 du Code de santé publique qui les définit comme « tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou en association, y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. Constitue également un dispositif médical le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostiques ou thérapeutiques. »

La définition du Code de santé publique semble en corrélation avec la définition des objets connectés qui permettent de « stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant. [623]». En effet, le régime des dispositifs médicaux serait une alternative permettant d'encadrer les applications de santé via l'utilisation de Smartphones. Un exemple de dispositif médical déjà dans le commerce en France est le système « Freestyle Libre[624] » qui permet à une personne atteinte de diabète de contrôler sa glycémie grâce à un capteur placé sous cutané. L'utilisation des capteurs entre dans le champ d'application du régime encadrant les dispositifs médicaux utilisés chez l'homme à des fins « de diagnostic, prévention, contrôle, traitement ou

---

[621] Ibidem.
[622] Ibidem.
[623] A. Mendoza-Caminade, « *Big data* et données de santé : quelles régulations juridiques ? », op cit loci.
[624] Le lecteur FreeStyle Libre exploite la technologie avancée des capteurs. Il offre la possibilité de scanner les données de glucose, puis immédiatement affiche les données d'une manière claire, lisible et facile à interpréter.

d'atténuation d'une maladie, d'une blessure ou d'un handicap ; d'étude, de remplacement ou modification de l'anatomie ou d'un processus physiologique ; de maîtrise de la conception.[625] ». Les dispositifs médicaux implantés dans ou sur le corps humain sont autonomes et permettent véritablement de calculer et d'assister la personne dans la prise en charge ou dans la prévention d'une pathologie. En outre, il convient d'insister sur le fait que ces objets et logiciels sont autonomes et ne donnent pas une visibilité très claire des données stockées et traitées par le dispositif. Ils ne sont pas toujours d'une grande fiabilité comme le remarque le Conseil National de l'Ordre des Médecins dans son livre blanc publié en janvier 2015[626].

La CNIL, quant elle, propose, sur le modèle de certification des hébergeurs, qu'une certification soit possible concernant les « objets connectés à visée médicale [627]».

188. L'expression du consentement.- Malgré les nombreuses lois concernant le commerce électronique, le législateur reste muet quant à la spécificité du consentement. Cela peut être justifié par la volonté de ne pas alourdir les procédures permettant l'expression d'un consentement libre et éclairé. Ce choix[628] peut aussi s'expliquer par la difficulté de mettre en place un formalisme unique qui risquerait de provoquer une entrave à l'innovation. De fait, il semble que le rôle du juge se verrait renforcé[629], permettant la protection des droits par « touches successives » et pouvant faire apparaître les caractères communs[630] d'un consentement réel et éclairé. Le rôle du juge sera renforcé dans sa recherche de moyens alternatifs permettant de réaliser une adaptation de la recherche du consentement notamment en se référant à des moyens extra-légaux, à défaut de conditions

---

[625] Ibidem note 609.

[626]Les applications et objets connectés de santé peuvent constituer des outils complémentaires utiles à la prise en charge des patients. Ils peuvent soutenir et renforcer la relation patient-médecin. Des dispositifs de m-santé, sous réserve de leur fiabilité, peuvent contribuer à améliorer l'adhésion des patients aux conseils de prévention, d'hygiène de vie et aux protocoles de soins, à faciliter les contacts entre les médecins et les patients. Livre blanc du conseil national de l'ordre des médecins « E-santé et santé connecté ».

[627] CNIL, « *Le corps nouvel objet connecté. Du quantified self à la m-santé : les nouveaux territoires de la mise en données du monde. »* Mai 2014.

[628] Si s'en est un.

[629] H.Herveg, « Panorama des responsabilités liées aux services et produits de santé en ligne en droit européen », *RDTI,* 2008, n°68 et s.

[630] Voir la critique de R. Lindon concernant le silence du Code civil sur la reconnaissance des droits la personnalité in « pour une pleine reconnaissance du droit à la protection des données à caractère personnel », J-M. Lacoste, thèse Toulouse Capitole 1, 2008.p71.

clairement identifiables[631]. Par exemple, vis-à-vis de l'information que doit délivrer le professionnel de santé afin que le patient puisse consentir, en connaissance de cause, à la collecte et à l'utilisation des données recueillies. Le juge pourra se référer au « guide du professionnel de santé » rédigé par la CNIL[632]. Il pourra également recourir à des chartes, à la doctrine ou à des déclarations[633]. Le nouveau Règlement Européen[634] invite, dans son article 38, « Les États membres, les autorités de contrôle et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des différents secteurs de traitement de données, à la bonne application des dispositions du présent règlement ».

D'un point de vue pratique, une simple pression de la souris paraît insuffisante pour manifester un consentement éclairé. En revanche, le système du « double clic » pourrait constituer une solution. En effet, la Loi de Confiance en l'Economie Numérique (LCEN)[635] consacre le principe du « double-clic » en exigeant « pour que le contrat soit valablement conclu », que le destinataire de l'offre ait eu « la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation » (par création, art. 1369-2 du Code civil). Sur le même principe du « double clic », le patient internaute devrait pouvoir être en mesure de vérifier les données de santé qu'il dépose et être informé de la finalité de leur traitement automatisé. Il convient également d'ajouter les apports de la proposition de Règlement européen du Parlement et de la Commission qui prévoit que la personne concernée par le traitement puisse avoir connaissance des tiers qui sont amenés à être associés au traitement. C'est-à-dire que la personne doit pouvoir clairement identifier l'arborescence des différents

[631] Relativement au consentement électronique, l'une des rares dispositions de nature législative que l'on peut identifier est la directive 2000/31/CE du 8 juin 2000 dont l'art. 10 s'intitulant « informations à fournir » évoque certaines mentions qui sont de nature à éclairer le consentement du consommateur Antérieurement, la directive européenne du 20 mai 1997 visant à instaurer une meilleure protection des consommateurs au niveau de l'Union Européenne, peut également être citée.

[632]CNIL,« le guide du professionnel de santé » 2011 disponible sur http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-uide_professionnels_de_sante.pdf

[633] Conseil National du Numérique – « rapport sur la neutralité des plateformes- Réunir les conditions d'un environnement numérique ouvert et soutenable » Mai 2014.

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

[635] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique JORF n°0143 du 22 juin 2004 page 11168.

acteurs rattachés à l'entreprise avec laquelle il a la volonté de partager ses informations ainsi que le rôle de chacun. C'est l'objet de l'article 43 du Règlement européen[636].

Freiner la vitesse de la transaction[637] semble être une solution viable pour assurer le consentement de la personne au traitement automatisé de ses informations. Cependant, compte tenu de l'opacité des contrats, des conditions d'utilisation et de l' « attrait du e-commerce[638] » en raison de sa rapidité, il semble que le système du « double-clic » incarne un concept de sécurité qui permettrait de diminuer les possibilités d'acceptations données par erreur ou par inadvertance. Cela donnerait un caractère « sincère[639]» au consentement. Ainsi T. Hassler affirme que « si la signature vient conforter le clic, on peut présumer que l'auteur de la signature est bien celui qui a émis le clic. De plus, la signature électronique revêt une supériorité par rapport à la signature manuscrite : elle ne peut être imitée, ce qui supprime, parmi d'autres, un risque possible de fraude[640]».

189. L'accès à une interface claire et accessible.- Le dernier plan d'action « 2012-2020 » de la Commission souligne que « Maintenant, plus que jamais, les gens surveillent leur santé et leur bien-être en ligne ou par des dispositifs tels que les smartphones. Le plan d'action reflète ce changement de comportement et vise à renforcer la confiance des utilisateurs dans ces outils numériques et des applications, tout en s'assurant que les conditions du marché encouragent l'innovation continue.[641]»

Il semble donc que le développement de la télésanté soit une réelle préoccupation à l'échelle européenne. La définition du cadre juridique des prestations de télésanté permettra d'en établir les règles de fonctionnement en termes de traitement de données de santé à caractère personnel qui seront traitées via les TIC. L'usage des TIC se coordonne parfaitement avec le projet de révision de la directive n°95 /46/CE du 24 octobre 1995.

---

[636] Règlement Du Parlement Européen Et Du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) p. 33.
[637] P-Y.Gautier et X. Linant de Bellefonds, « De l'écrit électronique et des signatures qui s'y attachent », J.C.P.G., n°24, 14 juin 2000, p.1116.
[638] Rapport d'information du sénateur Joël Bourdin- « Le commerce électronique, l'irrésistible expansion ». www.senat.fr.
[639] Maître A. Caprioli « De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ?». Disponible sur http://www.uncitral.org/pdf/english/colloquia/EC/Caprioli_Article.pdf
[640] T . Hassler, « Preuve de l'existence d'un contrat et Internet» (7 juillet 1999), p. 143, en ligne: Juriscom.net : http://www.juriscom.net/pro/l/signI9990716.htm
[641] Traduit de l'Anglais *: European Commission*, Memo, Brussels, 7 Décembre 2012.

Il est important de rappeler certains textes fondamentaux tels que l'article 8 de la Convention Européenne de Sauvegarde Des Droits de l'Homme et des Libertés Fondamentales[642] et la Convention du Conseil de l'Europe STE n°108 du 28 janvier 1981 relatifs au traitement automatisé des données à caractère personnel.

Le principe d'interdiction de traiter les données sensibles posé par l'article 8, paragraphe 1, de la directive 95/46/CE et l'article 6 de la Convention du Conseil de l'Europe connaissent des exceptions, notamment lorsqu'il s'agit de dispenser au patient les soins les plus appropriés[643] ou lorsque sa vie est en danger. C'est également le cas lorsque la personne est hors d'état de manifester sa volonté. Cette disposition permettrait au praticien d'accéder aux informations stockées dans le dossier médical électronique du patient afin d'en extraire les informations qui lui permettraient d'administrer un soin ou un traitement adéquat.

190. La question du consentement du patient au traitement de ses données est donc critique. Le Groupe de Travail de « l'article 29 » concernant le DMP, recommande que : « le patient devrait toujours avoir la faculté, s'il le désire, d'interdire la communication de ses données médicales, rassemblées par un professionnel de santé durant le traitement, à d'autres professionnels de santé ». C'est la difficulté que pose le droit de masquage qui donne la faculté à la personne de masquer totalement ou partiellement les informations. Cette problématique est centrale, notamment en termes de responsabilité médicale.

Il faut retenir que, de manière générale, tous les Etats Membres doivent limiter - sur le fondement du principe de finalité légitime du traitement - « le partage d'informations à ce qui est nécessaire pour la réalisation par chacun de ses propres fonctions et enfin un partage de l'information entre les professionnels liés par le secret médical. ». Ces règles concernent les prestations qui sont faites dans l'UE.

Pour le cas où les données doivent faire l'objet d'un transfert vers un pays tiers, chaque Etat Membre peut autoriser ce transfert si l'Etat destinataire dispose des garanties suffisantes de sécurité et de confidentialité concernant l'échange de données sensibles à caractère personnel[644]. Cela passe nécessairement par la mise en place d'une information

[642] Convention du Conseil de l'Europe adoptée à Rome le 4 nov. 1950.
[643] Art. 8, § 2, de la directive 95/46/CE. Op. Cit.
[644] Article 26 de la directive n°95/46/CE du 24 octobre 1995 op. cit. loci.

claire. C'est également ce qu'a affirmé la commission LIBE au sujet de l'information délivrée à la personne concernée, qui passe notamment par une « signalétique ».

L'article 11 §2 vise la « standardisation de l'information des personnes » du projet européen et prévoit que « le responsable du traitement applique des règles internes transparentes et facilement accessibles en ce qui concerne le traitement des données à caractère personnel et en vue de l'exercice de leurs droits par les personnes concernées. »

La Commission LIBE complète le projet européen en ajoutant « la nécessité de fournir cette information sous format d'icônes tout en réservant à la Commission Européenne le pouvoir de définir leur contenu par la voie d'actes délégués »[645]. L'objectif de la Commission est de rendre complètement accessibles et compréhensibles les documents d'information et les conditions de traitement de leurs données grâce à l'intégration d'icônes permettant de savoir qui pourra accéder aux informations[646]. Selon la commission LIBE, le responsable du traitement devra faire figurer un certain nombre d'icônes clairs permettant de connaître la finalité de chaque information recueillie, de son éventuelle conservation ainsi que de son éventuel partage avec des tiers. Par exemple, lors du remplissage d'un formulaire, nous pouvons imaginer qu'à côté de la ligne où l'utilisateur devra renseigner son nom, un icône fera apparaître un message lui permettant d'identifier toutes les personnes qui auront accès à ce renseignement.

Conclusion.- La neutralité de la collecte des données de santé, et plus généralement des données à caractère personnel doit être assurée par : la combinaison des obligations pesants sur le responsable du traitement et la garantie de la mise en œuvre des moyens sécurisés, tels que les processus d'anonymisation, lors des opérations de traitement.

[645] *Réforme du cadre européen de la protection des données à caractère personnel : où en est-on* ?, N. Métallinos et N. Botchorichvili, Avocate Bird & Bird, Revue Lamy, Droit de l'Immatériel, 2013 page 99.
[646] Voir annexe n° 2.

En janvier 2012, la Commission Européenne a proposé une réforme des règles en matière de protection des données dans l'Union Européenne. L'objectif des nouvelles règles est de redonner aux citoyens le contrôle de leurs données personnelles.

De plus, la reconnaissance des droits transfrontaliers en matière de soins justifie une mise en place d'un cadre renforcé de la collecte des informations, notamment en permettant aux entreprises de prévoir un niveau de sécurité plus élevé tout en permettant une maîtrise renforcée du flux d'informations par la personne concernée par le traitement de ses informations personnelles.

La Commission Européenne est actuellement en train de réformer le cadre juridique général de l'UE sur la protection des données personnelles. Les principaux objectifs de la Commission sont les suivants : moderniser le système juridique de l'UE pour la protection des données personnelles, en particulier pour relever les défis résultant de la mondialisation et du développement des nouvelles technologies ; renforcer les droits des individus, et, en même temps, réduire les formalités administratives afin d'assurer une libre circulation des données personnelles au sein de l'UE et au-delà ; améliorer la clarté et la cohérence des règles de l'UE pour la protection des données personnelles et réaliser une application cohérente et efficace de l'application du droit fondamental à la protection des données personnelles dans tous les domaines d'activités de l'Union.

Cette évolution au niveau européen est aussi l'objet d'une réflexion de la part de notre législateur. En effet, depuis trois ans le gouvernement et la secrétaire générale Axelle Lemaire ont présenté le nouveau projet de « loi numérique » visant à instaurer une « République Numérique ». Le projet de loi entreprend la démarche de modifier les infrastructures étatiques pour donner corps à une « République Numérique » en phase avec les pratiques et outils de son temps, d'une part, et instaurer une « économie de la donnée » « pertinente, respectueuse de la personne et économiquement efficace, d'autre part ». Dans sa forme actuelle, « le texte prétend instaurer les conditions d'une liberté accrue pour la circulation des données et du savoir, d'une égalité de droits pour les usagers du net ce qui pose des questions relatives aux modèles économiques viables sur les réseaux, à la neutralité des acteurs du net (et pas seulement des Fournisseur d'Accès Internet), au droit à l'oubli et à la protection de la vie privée, d'une ouverture optimale au bénéfice des internautes tendant à ce que les règles d'accessibilité soient généraliser, et au-delà, le droit à une connexion web est en passe d'être promu, non encore au niveau constitutionnel

(même si on peut considérer que les débats et la décision du Conseil Constitutionnel relative à la loi Hadopi ont déjà entériné ce point), mais, déjà, au niveau légal [647]».

Le projet de loi numérique et le nouveau règlement européen ont pour objectifs principaux de donner ou de renforcer les droits des personnes en développant des outils technologiques en adéquation avec les principes juridiques fondamentaux renforçant l'exercice des prérogatives de la personne concernée par le traitement informatique (Partie2).

[647] A. Lemaire, Echange d'Axelle Lemaire, Secrétaire d'Etat au Numérique, 6 octobre 2015, www.republique-numerique.fr.

Partie 2 : Le renforcement de la protection assurant une maîtrise des données de santé à caractère personnel

L'évolution des moyens de traitement des données personnelles ne permettent pas toujours d'assurer une protection des données en amont du traitement. La protection des données après le traitement est cruciale afin d'assurer la protection des droits de la personne dans le temps. Cet enjeu est matérialisé par la nécessité de garantir un droit à l'information de la personne, dont l'effectivité conditionne la portée du consentement (Titre 1). Cet enjeu a également incité la Commission et le Parlement à l'élaboration du nouveau Règlement Européen du 27 avril 2016, relatif à la protection et la circulation des données à caractère personnel, qui sera applicable en 2018 et abrogeant la directive 95/46/CE (Titre 2).

Titre 1 : La protection des données après le traitement

La première garantie des droits de la personne posée par la loi «Informatique et Libertés» de 1978 se traduit sous la forme d'une obligation imposée au maître du traitement. Il s'agit de l'obligation d'information qui garantit le droit à l'information de la personne concernée par le traitement informatique de ses données (Chapitre 1). Le droit à l'information et le droit d'accès aux informations permet ainsi la garantie de droits qui en découlent comme le droit de rectification et le droit d'effacement dont les modalités d'exercice ont fait l'objet d'une évolution notamment avec la consécration d'un droit à l'oubli numérique initié par l'arrêt *Google Spain* (Chapitre 2).

Chapitre 1 : Le droit d'accès aux informations

L'obligation d'information trouve son fondement à l'article 27 de la loi «Informatique et Libertés» du 6 janvier 1978. C'est la directive 95/46/CE qui vient compléter son contenu ainsi que son champ d'application (Section 1). Le droit à l'information a pour corollaire le droit d'accès dont l'origine se trouve à l'article 39 de la loi «Informatique et Libertés» et dont le champ d'application est large. Erigé en droit fondamental, le droit d'accès permet l'exercice de prérogatives telles que les droits d'accès et d'opposition (Section 2).

Section 1 : Le droit à l'information

Le droit à l'information est considéré comme un véritable droit fondamental de la personne. La CNIL est extrêmement rigoureuse en ce qui concerne le contenu (a) et les modalités d'accomplissement de cette obligation (b). De plus, les dérogations autorisant à ne pas informer la personne concernée ont fait l'objet de nombreux avis de la Commission qui a mis au point des techniques très précises en matière de sécurité (c).

a) Le contenu de l'obligation

Lorsque la loi «Informatique et Libertés» a été votée, il est apparu que le droit à l'information de la personne concernée par le traitement était un droit fondamental[648]. En effet, les personnes devaient être averties des conséquences de la collecte des informations les concernant et du caractère obligatoire ou facultatif de leur réponse[649]. Elles devaient être informées de l'identité des destinataires (personne physique ou morale), et cette information devait être assortie de l'existence d'un droit d'accès et de rectification.

Lors de la transposition[650] de la directive européenne 95/46/CE, les articles 10 et 11 envisageaient un cas qui n'était pas visé par la loi «Informatique et Libertés» de 1978, en l'occurrence, le cas des données qui étaient collectées de façon indirecte. Cette modalité de

[648] Cf. Rapport Tricot op. cit. loci.
[649] Article 27 ancien de la loi «Informatique et Libertés».
[650] Article 32 I, de loi «Informatique et Libertés» modifiée.

collecte a donc été transposée en droit interne à l'article 32 §I[651]. Cependant, les articles 10 et 11 ne prévoyaient la transmission des autres informations que dans certaines circonstances[652]. Cela qui a été interprété par le G29 comme un risque de *désharmonisation* des moyens d'information de la personne concernée par le traitement[653].

191. La portée de l'obligation d'information.- L'obligation est considérée comme un droit de la personne ; c'est-à-dire que le responsable est le débiteur de cette obligation. Cette obligation permet d'avoir connaissance des données qui sont traitées et une maîtrise de celles-ci par la personne concernée. Le droit à l'information est fondamental compte tenu de « l'amoindrissement du contrôle a priori [654]». l'obligation d'information est la garantie d'un « traitement loyal », lequel « suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées directement auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte[655] ». Elle permet aux personnes de pouvoir exercer pleinement leurs droits d'opposition et d'accès aux informations les concernant (que nous ne traiterons pas ici[656]). L'obligation d'information diffère selon que les informations ont été collectées directement ou indirectement[657]. Ensuite, depuis la transposition de la directive 2009/136/CE du 25 novembre 2009[658], la loi «Informatique et Libertés» prévoit l'application d'un régime spécifique en matière de traitement par un service de communications électroniques.

192. Le régime applicable en cas de collecte directe.- Les informations que doit communiquer le responsable du traitement sont visées à l'article 32 §I de la loi «Informatique et Libertés» modifiée. Le législateur a ainsi effectué la transposition de

---

[651] Voir Supra « la notion de légitimité du traitement » p147.
[652] Les informations relatives aux destinataires, le caractère obligatoire ou facultatif des réponses doivent être appréciés en considération « des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données » article 10 c) et 11 c) de la directive européenne 95/46/CE op. cit. loci.
[653] G29, Avis 10/2004, WP 100, adopté le 25 novembre 2004, relatif aux dispositions davantage harmonisées en matière d'information.
[654] N.Mallet-Poujol, , « Quels droits pour l'individu face au risque d'un Etat Big Brother ? », Cahiers Français, « La place de l'Etat aujourd'hui », Documentation française n°379, mars-avril 2014, pp. 59-65
[655] Directive européenne 95/46/CE op. cit. loci. Considérant n°38.
[656] Cf infra p 202.
[657] Article 32 §I de la loi «Informatique et Libertés» modifiée op. cit. loci.
[658] Journal Officiel de l'Union Européenne du 18 Décembre 2009

l'article 10 de la directive 95/46/CE de 1995 en complétant les exigences prévues par l'ancien article 27 de la loi «Informatique et Libertés» de 1978. Le législateur français a ajouté la prise en compte du caractère obligatoire ou facultatif des réponses, les conséquences éventuelles d'un défaut de réponse, les destinataires des données et l'existence d'un droit d'accès, d'opposition et de rectification.

Le législateur français n'a donc pas repris la totalité de la directive et a visé sept informations qui doivent obligatoirement être communiquées à la personne concernée par le traitement[659]. En effet, la directive fait une distinction entre les informations essentielles telles que l'identité du responsable, la finalité du traitement et les informations qui doivent être complémentaires compte tenu des circonstances particulières, comme le prévoit le considérant 38 de la directive. La transposition en droit interne ne prévoit l'application de certaines dispositions que dans certains cas [660]: lorsque les données sont collectées via un questionnaire, le législateur a réduit le nombre d'informations minimales à fournir visées par l'article 32 alinéa 2 de la loi «Informatique et Libertés» de 1978 modifiée, et prévoit que le responsable ne doit fournir *que* quatre informations jugées essentielles par la CNIL[661], à savoir :

« - l'identité du responsable de traitement ou de son représentant ;

- la finalité de ce traitement ;

- le caractère obligatoire ou facultatif des réponses ;

- et, les droits dont les personnes concernées disposent en matière d'opposition, d'accès et de rectification et de suppression de leurs données.[662] »

[659] A savoir : l'identité du responsable du traitement et, le cas échéant, celle de son représentant ; la finalité poursuivie par le traitement auquel les données personnelles sont destinées ; le caractère obligatoire ou facultatif des réponses ; les conséquences éventuelles, à l'égard de la personne concernée, d'un défaut de réponse de sa part ; les destinataires ou catégories de destinataires des données personnelles en cause ; les droits d'opposition, d'accès, de modification et de suppression, dont dispose la personne concernée au titre de la loi «Informatique et Libertés» ; ainsi que, mais uniquement le cas échéant, si les données personnelles font l'objet d'un transfert hors de l'Union européenne, d'autres précisions devant, dans ce cas, être communiquées.

[660] Transposition de l'article 10 de la directive européenne 95/46/CE

[661] CNIL, 6e rapport annuel d'activité 1985 : Doc. fr., 1986, p. 362 ; délibération n° 2014-139, autorisant le Conseil Général de la Haute-Marne à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des dossiers traités dans les domaines de l'aide sociale et de l'allocation personnalisée d'autonomie aux personnes âgées, 3 avril 2014.

[662] Loi «Informatique et Libertés» de 1978 modifiée, article 32, I, al. 1er, 1°, 2°, 3° et 6°.

Ces informations doivent êtres communiquées à la personne concernée par le traitement à l'écrit ou à l'oral. Lorsque la communication se fait oralement, la CNIL exige que la personne soit préalablement informée par courrier des mentions obligatoires[663].

193. Les précisions en cas de transfert vers un pays tiers.- Le décret n° 2005-1309 du 20 octobre 2005 prévoit la communication d'informations complémentaires en cas de transfert vers un pays tiers. L'article 90 alinéa 1[er] impose au responsable du traitement de fournir :

« - le ou les pays d'établissement du destinataire des données dans les cas où ce ou ces pays sont déterminés lors de la collecte des données ;

- la nature des données transférées ;

- la finalité du transfert envisagé ;

- la ou des catégories de destinataires des données ;

- le niveau de protection offert par le ou les pays tiers. »

Enfin, le législateur, dans un souci de protection optimale, a prévu l'ajout de deux conditions en cas de transfert vers un pays tiers. En effet, le décret d'application de 2005[664] prévoit que soit communiquée à la personne concernée[665] :

« - soit la décision de la Commission européenne autorisant le transfert, si le ou les pays tiers destinataires du transfert figurent sur la liste des États ayant fait l'objet d'une décision de la Commission européenne reconnaissant qu'ils garantissent un niveau adéquat de protection des données personnelles au sens de la directive du 24 octobre 1995;

- soit l'exception prévue à l'article 69 de la loi modifiée du 6 janvier 1978 qui permet ce transfert ou la décision de la CNIL autorisant ce transfert, si le ou les pays tiers ne satisfont pas aux conditions prévues à l'article 68 de cette loi. »

---

[663]CNIL, Délibération n°2013-259, autorisant l'Institut National de la Prévention et de l'Education pour la Santé (INPES) à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité l'étude des caractéristiques socio-économiques des ménages intoxiqués par le monoxyde de carbone de façon accidentelle dans leur habitat et de leur niveau de connaissance quant aux risques d'exposition à ce gaz, 19 septembre 2013, Légifrance.

[664] Décret n°2005-1309 du 20 octobre 2005, pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. JORF 22 oct. 2005.

[665] Jur.Cl. Administratif, Fasc. 274-30 : Informatique. Données à caractère personnel. Formalités préalables à la mise en œuvre d'un traitement de données à caractère personnel §100 et suivant.

Enfin, si le responsable envisage le transfert des données vers un pays tiers postérieurement à la collecte des données, l'article 91 du décret d'application n°2005-1309 dispose que le responsable du traitement a un délai de quinze jours pour faire parvenir les informations à l'intéressé.

194. L'obligation d'information en cas de collecte indirecte.- L'ancienne rédaction de la loi «Informatique et Libertés» ne prévoyait pas un régime de protection de la personne concernée en cas de collecte indirecte de ses informations[666]. La collecte indirecte entraînait une difficulté en ce sens où la CNIL et la Cour de Cassation n'avaient pas la même interprétation de l'obligation d'information en cas de collecte indirecte. En effet, la CNIL avait une interprétation très large de l'obligation d'informer et considérait que le cessionnaire se subrogeait à l'obligation du cédant[667]. Or, la Cour de Cassation avait une interprétation plus lapidaire eut égard à « l'absence de dispositions expresses » faisant peser sur le responsable du traitement (cessionnaire) l'obligation d'informer la personne concernée[668]. Ainsi, l'article 32 III de la loi «Informatique et Libertés» reprend l'article 11 de la directive européenne du 24 octobre 1995. Le législateur français renforce le cadre de la protection des données personnelles collectées indirectement. Cette protection se justifie notamment en raison de la multiplication des cessions de banques de données entre entreprises ou à des fins de prospections commerciales[669]. A la lecture du considérant 39 de la directive européenne 95/46/CE, on constate que l'encadrement de ces pratiques n'est pas un frein à la communication d'informations postérieure à un tiers mais une volonté de la part du législateur européen de préserver les dynamiques économiques, tout en préservant les droits et libertés des personnes. Ainsi, l'article 32 §III de loi «Informatique et Libertés» de 1978 modifiée permet d'encadrer la cession de fichiers client et de préserver les données collectées, notamment via des sites publics[670]. Par conséquent, le

---

[666] Rapport n° 218 (2002-2003) de M. A. Türk, fait au nom de la commission des lois, déposé le 19 mars 2003, disponible sur le site sénat.fr.
[667] CNIL, 7e rapport annuel d'activité 1986 : La Doc. fr., 1987, p. 75.
[668] Cass. crim., 25 oct. 1995, n° 94-85.781, Bernard X: *JurisData* n° 1995-003536 ; Bull. Lamy févr. 1996, p. 6.
[669] Rapport 218 du 19 mars 2003, op. cit. loci.
[670] CNIL, Délibération n°2009-203, formation restreinte prononçant une sanction pécuniaire à l'encontre de la société *Directannonces*, du 26 février 2009 ; Voir aussi délibération n°2011-203 portant avertissement à l'encontre de la société Pages Jaunes, du 21 septembre 2011 : En l'espèce, la formation restreinte de le CNIL qualifie de déloyale la collecte de données lorsque une société *« prévoit d'aspirer les profils issus des réseaux sociaux sur Internet sans que les personnes concernées en aient été préalablement informées. »*

responsable du traitement « ou son représentant » doit fournir toutes les informations visées à l'article 32 §I de la loi «Informatique et Libertés» modifiée dans les mêmes conditions que celles prévues lorsqu'il s'agit d'une collecte directe de données[671].

195. La collecte de données par un service de communication électronique.- L'analyse de la collecte d'informations dans le domaine des communications électroniques s'impose compte tenu du développement et de l'évolution des moyens de collecte. L'obligation d'information lors de l'utilisation d'un service de communication est issue de la transposition de la directive 2002/58/CE du 12 juillet 2002 concernant le « traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques » modifiée par la directive 2009/136/CE du 25 novembre 2009 dont l'objectif principal était de réglementer l'installation des cookies sur le terminal des utilisateurs et d'imposer de nouvelles obligations aux opérateurs en cas de violation des données à caractère personnel[672].

196. L'évolution du cadre juridique.- Dans un premier temps, la directive du 12 juillet 2002 visait essentiellement une information *claire et précise* des personnes concernées par le traitement, mais aucun type d'actions positives permettant de déduire le consentement de la personne ne figurait dans la première version de la directive. En d'autres termes, seule l'information indiquant la collecte des données de la personne suffisait. Cette information devait indiquer à la personne « la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion » et les « moyens dont elle dispose pour s'y opposer [673]». Ainsi, l'article 32 §II alinéa 2 de la loi «Informatique et Libertés», dans sa version issue de la loi de 2004, transpose l'article 5 de la directive du 12 juillet 2002[674] et

---

[671] CE, ord. réf., 5 sept. 2008, n° 319071, Sté *Directannonces* : JCP E 2009, 1674 ; Gaz. Pal. 10 oct. 2009 n° 283, p. 5, note G. Haas et L. Goutorbe ; et voir aussi récemment la confirmation CE, 23 mars 2015, n° 357556, Sté Groupe DES France : *JurisData* n° 2015-006507 ;

[672] Directive 2009/136/CE du 25 novembre 2009 « *Le contrat avec le client devrait aussi préciser le type de mesure éventuelle que le fournisseur pourrait prendre afin de réagir à un incident ayant trait à la sécurité ou à l'intégrité ou de faire face à des menaces ou à des situations de vulnérabilité.* » considérant 25. De même le considérant 65 dispose qu' « *Il convient d'assurer un niveau élevé de protection de la sphère privée qui soit équivalent pour tous les utilisateurs* »

[673] Loi «Informatique et Libertés» n°78-17, modifiée par la loi n°2004-801 du 6 août 2004.

[674] « Les États membres garantissent que l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur, soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre

prévoit que le stockage ou l'accès technique au terminal de la personne est autorisé, si cet accès a pour finalité « exclusive » de permettre la transmission d'une communication par voie électronique. Cet accès doit aussi avoir a pour objectif de faciliter une telle transmission, ou, l'opération doit être strictement nécessaire à la fourniture d'un service expressément demandé par l'utilisateur. Devenue *obsolète* en raison de l'évolution des moyens technologiques et de traitements des données, la directive 2009/136/CE du 15 novembre 2009 a été transposée en droit interne par la l'ordonnance n°2011-1012 du 24 août 2004[675] modifiant l'article 32 de loi «Informatique et Libertés» de 1978 modifiée par la loi 6 août 2004.

197. L'extension du champ d'application.- La transposition de la directive du 24 août 2009 permet l'application de la protection en incluant les personnes morales. En effet, à l'origine, la protection s'appliquait à « toute personne utilisatrice » alors que la nouvelle rédaction de l'article 32 de la loi «Informatique et Libertés» vise « tout abonné » à un service de communication. En ce qui concerne les conditions d'application, la CNIL affirme que les dispositions s'appliquent aux informations « stockées et consultées », que ces données soient à caractère personnel ou non[676]. La Commission reprend l'avis du G29, rendu le 22 juin 2010, qui affirme que les dispositions s'appliquent dans un but de protection de la vie privée et que la nature des informations « importe peu[677] ».
Enfin, l'article 32 de la loi «Informatique et Libertés» de 1978 modifiée par l'ordonnance n°2011-1012 prévoit que l'application des dispositions de la loi s'applique à tous les « équipement[s]terminal[aux]». Comme le font remarquer certains auteurs, il faut interpréter cette notion par « référence au Code des postes et des communications

autres sur les finalités du traitement, et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. » Article 5, 3) de la directive européenne 12 juillet 2002 Journal officiel *n° L 201 du 31/07/2002 p. 0037 – 0047*.

[675] Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques JORF du 26 août 2011.

[676] CNIL, délibération n°2013-378 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978, du 5 décembre 2013, JORF n°0299 du 26 décembre 2013.

[677] G29, avis n°2/2010 du 22 juin 2010, WP171.

électroniques » qui transpose l'essentiel de la directive 2002/58/CE du 12 juillet 2002[678]. Il convient de relever que le champ d'application est large et d'en déduire que le texte de loi a pour objectif de couvrir un maximum de cas de stockages et d'utilisations des données personnelles ; comme le constate la CNIL qui énumère toutes les formes d'utilisation de terminaux impliquant la collecte des données personnelles telles que les « logiciels ou [d'une] application mobile, quel que soit le système d'exploitation, le navigateur ou le terminal utilisés (par exemple, un ordinateur, une tablette, un ordiphone ou "Smartphone", une télévision connectée, une console de jeux vidéos connectée au réseau Internet) »[679].

198. L'obligation d'information dans le cadre des recherches médicales.- Les données collectées/traitées à des fins médicales sont visées à l'article 8 §I de la loi «Informatique et Libertés» modifiée et font l'objet d'un encadrement spécifique en raison de leur caractère sensible. Lorsqu'un responsable du traitement souhaite mettre en place un traitement aux fins de recherche médicale, il doit se conformer aux obligations disposées à l'article 32 de loi «Informatique et Libertés» modifiée et informer la personne concernée par le traitement en se conformant aux dispositions relatives aux transferts des données visés aux articles 90 et 91 du décret d'application précédemment cités. En matière d'information de la personne concernée par un traitement de données à des fins de recherche médicale, le responsable du traitement doit informer individuellement la personne. L'article 57 de la loi «Informatique et Libertés» de 1978 modifiée par la loi de modernisation de notre système de santé du 26 janvier 2016[680] dispose que l'information doit parvenir avant même de commencer le traitement. Ainsi, le responsable du traitement devra communiquer :

> « 1° La nature des informations transmises ;
>
> 2° La finalité du traitement de données ;
>
> 3° Les personnes physiques ou morales destinataires des données ;
>
> 4° Le droit d'accès et de rectification institué aux articles 39 et 40 ;
>
> 5° Le droit d'opposition institué aux premier et troisième alinéas de l'article 56 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement. »

[678] R. Perray, Données à caractère personnel, introduction générale et champ d'application de la loi «Informatique et Libertés», Juris-classeur administratif, fascicule 274-10, n°°24 et s. 30 juillet 2014.
[679] CNIL, délibération n°2013-378 op. cit. loci.
[680] Loi n°2016-41 du 26 janvier 2016 - art. 193.

Compte tenu du caractère spécifique du traitement des données de santé à caractère personnel, le décret d'application n°2007-451[681] du 25 mars 2007 prévoit que les personnes concernées par le traitement de données personnelles aux fins de recherches médicales ou « dans le domaine de la santé sont informées, des mentions prescrites par l'article 57 de la loi du 6 janvier 1978 susvisée, par la remise d'un document ou par tout autre moyen approprié. » Il ressort du décret d'application que le responsable du traitement a une obligation d'information *renforcée* similaire à celle visée à l'article L.1111-2 du Code de santé publique, qui impose au praticien d'informer son patient de façon claire et précise.

b) Les modalités de l'information

199. Les informations doivent être communiquées sur le support qui est à l'origine de la collecte, et, le cas échéant, doivent être transmises via un document porté à la connaissance de personne concernée par le traitement[682]. Lorsque cette information est communiquée par un document, elle doit être inscrite en caractère lisible. L'information doit mentionner les coordonnées du service auprès duquel la personne concernée par le traitement peut exercer son droit d'accès, d'opposition et de rectification. Dans le cas particulier où la collecte des données est effectuée oralement, la formation restreinte de la CNIL précise que les informations précédemment citées doivent être notifiées à l'intéressé. Elle ajoute que la personne concernée doit pouvoir être informée sur simple demande orale et recevoir les informations par écrit postérieurement à la collecte[683]. Il incombe également au responsable du traitement d'informer la personne concernée par le traitement qu'il peut transmettre ses informations par voie électronique.

200. La position de la CNIL.- La CNIL est très attentive à ce que l'obligation d'information soit respectée tant dans ses conditions de garantie que dans ses modalités. A ce propos, la doctrine de la Commission est riche en matière de modalités d'information de

[681] JORF 28 mars 2007.
[682] Décret n°2005-1309, article 90 op. cit. loci.
[683] CNIL, délibération n°2011-193, prononçant une sanction à l'encontre de la société *PM Participation,* dans laquelle elle demande à la société la preuve de l'exécution complète de l'obligation d'information. 28 juin 2011.

la personne concernée. Elle fait référence *au moment* et aux modalités de l'information dans ses nombreuses délibérations[684], mais elle anticipe également cette obligation dans ses nombreux guides et recommandations destinés aux professionnels : pour la prospection commerciale, les professionnels de la santé, en matière d'éducation, dans l'enseignement supérieur, la recherche et d'assurance[685].

La Commission est très vigilante vis-à-vis du respect de l'article 32 de la loi «Informatique et Libertés» modifiée qui impose de délivrer une information individuelle. Elle effectue une évaluation que l'on pourrait considérer au *cas par cas ;* par exemple ; elle considère que l'obligation d'information est remplie lorsque les personnes concernées sont avisées par courrier et que les professionnels peuvent l'être par voie d'affichage[686]. La CNIL considère que la communication d'informations générales assortie d'une information individuelle est plus protectrice[687].

Cette position est partagée par les juridictions administratives et judiciaires. En effet, la Cour d'Appel de Dijon indique qu'il appartient au maître du traitement de mettre œuvre toutes les mesures visant à informer la personne concernée par le traitement, de façon individuelle et que la charge de la preuve de l'accomplissement de ces mesures revient au maître du traitement[688]. De même, la Cour d'Appel de Lyon ne considère pas que l'obligation d'information soit remplie concernant la formation à l'usage d'un logiciel de suivi commercial qui ne précise pas, clairement, que les informations seront utilisées à des fins disciplinaire[689]. Il semble qu'aucun formalisme ne soit imposé tant que l'information est délivrée de façon claire et lisible. En effet, la CNIL considère que les caractères de l'information doivent être d'une taille « raisonnable »[690]. De même, la Commission avait indiqué que les informations concernant les données comportementales visant évaluer les

---

[684] CNIL, délibération n°2012-434, portant avis sur un projet de décision relative au traitement de gestion de la scolarité des étudiants mis à disposition par l'AMUE, 6 décembre 2012.
[685] Respectivement : CNIL, guide : « La pub, si je veux »2011 ; « professionnels de santé », 2011 ; «Informatique et Libertés» pour l'enseignement du second degré 2010, «Informatique et Libertés» pour l'enseignement supérieur, 2011 ; « pack de conformité » assurance, 2014. Médiathèque de la CNIL disponible sur www.cnil.fr.
[686] CNIL, délibération n°2013-210, autorisant la ville de Lyon à effectuer un traitement des données à caractère personnel en matière de sinistre, 11 juillet 2013.
[687] CNIL, délibération n°2013-157 autorisant la mise en œuvre d'un traitement des données à caractère personnel dans un EPAHD dont l'objectif est de faciliter les démarches d'admission des personnes âgées ; Délibération n°2013-233 autorisant le Crédit Agricole à mettre un traitement de données à caractère personnel pour lutter contre la fraude bancaire, 23 mai 2013.
[688] CA de Dijon, 23 février 2012, n°11/00083, *JurisData* n°2012-004128.
[689] CA Lyon, 14 avril 2011, affaire n°10/03759 *JurisData* n°2011-009603.
[690] CNIL, délibération n°01-040 relative aux fichiers Canal +, du 28 juin 2001.

comportements dans les ménages devaient être indiquées de façon claire et précise[691]. Si le caractère lisible de l'information ne doit pas correspondre à une police ou une à taille de lettres précise, la CNIL exige que la totalité des informations soient mentionnées[692] à chaque traitement des données.

c) Dérogations à l'obligation d'information

201. Collecte directe ou indirecte les dérogations communes.- L'article 32 IV, alinéa 1[693], alinéa 2[694], alinéa 3[695] et l'article 67[696] visent les cas où le responsable du traitement peut déroger à l'obligation d'information.

L'anonymisation à bref délai[697], présentation.- L'anonymisation à bref délai concerne notamment le traitement des données dans le secteur de la santé. C'est-à-dire que ce procédé renvoie à l'article 8 §III de la loi «Informatique et Libertés» concernant le traitement des données « sensibles ». La loi prévoie que l'anonymisation à bref délai doit être réalisée avec un procédé irréversible, approuvée par la CNIL et être immédiate[698]. Sur les procédés d'anonymisation, la Commission insiste sur le fait que les procédés doivent faire l'objet d'une vigilance accrue et d'une harmonisation pour éviter une dispersion de règles ayant des « effets comparables[699] ». Elle rappelle, en effet, que « le projet de loi relatif à la santé[700] prévoit déjà, pour les traitements de données de santé, que la Commission ait la possibilité d'homologuer et publier des méthodologies générales ou des

---

[691] CNIL, délibération n°97-012 relative à la segmentation comportementale sur les habitudes comportementales de consommation des ménages, 18 février 1997.
[692] CNIL, autorisation unique n°004, Délibération n° 2014-042 du 30 janvier 2014 modifiant l'autorisation unique n°2005-305 du 8 décembre 2005 n°AU-004 relative aux traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, voir aussi Cass. Soc., 8décembre 2009, n°08-17191, Comm. Com. électr. 2010 comm. 51, observation Lepage.
[693] L'anonymisation à bref délai.
[694] Traitement ayant pour objectif la prévention, la recherche, la constatation d'infractions pénale.
[695] L'information préalable de la personne.
[696] Les traitements aux fins de journalismes, d'expression littéraire et artistique.
[697] Article 25 §I 1°) de loi «Informatique et Libertés»
[698] CNIL, délibération n° 2015-414 du 19 novembre 2015 portant avis sur un projet de loi pour une République Numérique. La Commission rappelle que « l'anonymisation consiste à utiliser un ensemble de techniques de manière à rendre impossible toute identification ou ré-identification des personnes, par quelque moyen que ce soit et de manière irréversible.
[699] CNIL, délibération 2015-414 op. cit. loci.
[700] Loi de modernisation du système de santé, du 26 janvier 2016 op. cit. loci.

procédés d'anonymisation préalablement à la mise à disposition de ces données ou jeux de données[701] ».

202. La notion de « bref délai », telle que prévue par le décret[702] d'application initial de la loi «Informatique et Libertés» impliquait que l'anonymisation devait durer 8 jours, or la CNIL a vigoureusement refusé que soit prévu un tel délai en affirmant que la notion de « bref délai » n'implique pas une « anonymisation […] ni de huit jours, ni de un mois, mais de quelques secondes voire quelques heures[703] ».

203. Concernant les techniques d'anonymisation, la CNIL indique, dans son guide de la « sécurité des données personnelles » de 2010, quels sont les procédés et techniques d'anonymisation[704]. Le G29 a également publié un avis[705] sur les techniques d'anonymisation où il indique que les données anonymisées ne doivent pas permettre l'individualisation, ni permettre une « corrélation » entre deux ensembles distincts de données et que les données ne doivent permettre aucune « inférence » ; c'est-à-dire qu'il n'est pas possible de déduire l'Information concernant une personne. La Commission ajoute que l'anonymisation impose de respecter deux procédés : « transformer les données pour qu'elles ne se réfèrent plus à une personne réelle » et « généraliser les données de façon à ce qu'elles ne soient plus spécifiques à une personne mais communes à un ensemble de personnes ».

---

[701] CNIL, délibération 2015-414 op. cit. loci.

[702] Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. NOR: JUSC0520586D.

[703] Délibération no2006-218 du 28 septembre 2006 portant avis sur le projet de décret modifiant le décret no2005-1309 du 20 octobre 2005 pris pour l'application de la loi no78-17 du6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi no2004-801 du 6 août 2004, page 5.

[704] Etre très vigilant dans la mesure où une ré-identification peut intervenir à partir d'informations partielles. Anonymiser une donnée personnelle en procédant comme suit : générer un secret suffisamment long et difficile à mémoriser appliquer une fonction dite à sens unique sur les données : un algorithme convenant pour une telle opération est un algorithme de hachage à clé secrète, tel que l'algorithme HMAC basé sur SHA-1. Si une donnée personnelle est anonymisée et non purement supprimée, il existe un risque de ré-identification. En l'absence d'un besoin de levée de l'anonymat, il faut prévoir de supprimer le secret afin de réduire ce risque. Dans l'hypothèse où le secret doit être conservé pour une éventuelle levée de l'anonymisation ou une finalité de corrélation entre différentes données, il faut prévoir de mettre en place des mesures organisationnelles pour garantir la confidentialité de ce secret. Les accès à celui-ci doivent être tracés.

[705] Communiqué de presse Article 29 Data protection Working Party.

204. Exemples de procédés approuvés par la Commission.- Dans le cadre de l'accès aux données issues des feuilles de soins électroniques, la Commission a appliqué les recommandations du rapport Babusiaux[706] qui indiquent que les données « ne viennent pas, sous leur forme nominative ». La CNIL a complété ce procédé en indiquant que l'anonymisation des données devait reposer sur « l'utilisation de boîtes noires » devant se présenter sous la forme « d'un dispositif matériel inviolable » qui devait être soumis à l'audit d'un « organisme extérieur[707] », c'est-à-dire que la sécurité est assurée par l'interconnexion de plusieurs tiers de confiance.

La CNIL a renforcé[708] ses exigences techniques en matière d'anonymisation lorsque la société CELTIpharm a souhaité réaliser une étude épidémiologique en utilisant les données des feuilles de soins électroniques. La Commission a donné l'autorisation de l'utilisation des données épidémiologiques sous la forme d'un tableau[709] qui indique les moyens techniques que la société CELTIpharm devra mettre en œuvre pour assurer un traitement sécurisé :

> *« Anonymisation : le dispositif mettra en œuvre à plusieurs reprises une fonction d'anonymisation irréversible à clé secrète de type FOIN basée sur une fonction de hachage de la famille SHA-2 (256 bits), référencée ci-après sous le nom de FOIN2.*
>
> *Les données d'identification du patient feront l'objet d'une double anonymisation FOIN2 : une première anonymisation sera réalisée par les organismes concentrateurs techniques (OCT) et une deuxième par la société CELTIPharm. La clé détenue par l'OCT n'est jamais portée à la connaissance de la société CELTIPharm.*

---

[706] Rapport Babusiaux, L'accès des assureurs complémentaires aux données de sante des feuilles de soins électroniques, 26 mai 2003, Page 67, Doc. Fr. Coll. Rapports Publics.

[707] En l'espèce, la Commission reprend le dispositif recommandé par le Rapport Babusiaux qui prévoit un dispositif d'organisation du système en « deux sous-systèmes séparés communiquant entre eux par le truchement d'un tiers de confiance », CNIL, délibération n°2009-687 autorisant la société Groupama à mettre en œuvre un traitement ayant pour finalité d'accéder, sous forme anonymisée, à l'information sur les défauts visuels des assurés figurant sur les demandes de prise en charge, du 10 décembre 2009.

[708] CNIL, délibération n°2011-246, autorisant la mise en œuvre par la société CELTIPharm d'un traitement de données à caractère personnel ayant pour finalité la réalisation d'études épidémiologiques à partir de données issues des feuilles de soins électroniques anonymisées à bref délai, du 8 septembre 2011, disponible sur le site www.legifrance.gouv.fr.

[709] On peut saluer la clarté de l'information de la Commission, qui semble non seulement faire preuve de pragmatisme, mais surtout cette présentation dénote une volonté de ne laisser aucune place à l'improvisation de la part de la société CELTIpharm.

Le même procédé ne peut pas être utilisé pour anonymiser l'identifiant des professionnels de santé puisqu'il n'est pas déchiffré par l'OCT. La société CELTIPharm utilisera des clés de déchiffrement remis par le GIE SESAM Vitale insérés dans une boite noire (HSM) pour déchiffrer cet identifiant. La société CELTIPharm n'a pas accès aux secrets contenus dans cette boite noire. Une fois le déchiffrement de l'identifiant du professionnels de santé réalisé, il lui sera substitué, à bref délai, un nouvel identifiant calculé avec FOIN2.

Les secrets cryptographiques détenus par la société CELTIPharm seront sur supports individuels sécurisés et protégés selon le principe de partage des connaissances, avec un quorum minimum de 3 personnes nécessaires à l'activation d'un secret.

- Sécurité : Les échanges réseaux réalisés dans le cadre de ce traitement seront chiffrés. Le système d'information fait l'objet de mesures de protection logique et physique. Une traçabilité des accès au système d'information par les utilisateurs sera réalisée. La société CELTIPharm mettra en œuvre une politique de sécurité formalisée qui sera mise à jour annuellement. Des audits de sécurité seront effectués de manière régulière. »

De même, la Commission a renforcé sa position en matière d'anonymisation en précisant que « le dispositif d'anonymisation » à bref délai doit être « irréversible » afin de « prévenir la ré-identification des personnes » dont les données sont contenues dans les feuilles de « résultats d'analyses de biologie médicale » par la société en charge du traitement et « les hébergeurs de données de santé agréés ». Ainsi, la CNIL reprend[710] trois phases pour que l'anonymisation à bref délai soit effective[711] : la première phase est une « pseudonymisation » des données d'identification, elle doit avoir lieu dès que celles-ci sont collectées chez le premier hébergeur de données, c'est alors qu'un identifiant anonyme et calculé par un second hébergeur de données agréé devra se « substituer aux données d'identification » et ce n'est qu'après cette phase que la société en charge du traitement pourra enregistrer et traiter les données transmises.

Dans les deux délibérations, la CNIL a indiqué les modalités pour délivrer l'obligation d'information une fois que les conditions énoncées seraient remplies :

« Des affiches de présentation du traitement seront apposées dans les pharmacies dans lesquels les professionnels de santé participant au dispositif exercent.

[710] CNIL, Guide « La sécurisation des données personnelles » op. cit. loci.
[711] CNIL, Délibération n° 2013-371, autorisant la société Carre Castan Consultants à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la réalisation de veilles et d'études épidémiologiques et médico-économiques à partir des feuilles de résultats d'analyses des laboratoires d'analyses médicales, du 28 novembre 2013.

Conformément aux dispositions de l'article 32-IV de la loi du 6 janvier 1978 modifiée, relatives aux traitements portant sur des données faisant l'objet à bref délai d'un procédé d'anonymisation au sens de l'article 8-III de la même loi, la note d'information se limite à préciser l'identité du responsable de traitement ainsi que la finalité du traitement de données projeté.

Un numéro de téléphone vert et une adresse électronique seront mis à la disposition du public pour obtenir toute information complémentaire concernant le traitement. [712]*»*

Par conséquent, il apparaît que l'anonymisation à « bref délai » ne permet de déroger que partiellement à l'obligation d'information. C'est-à-dire que le responsable est *autorisé* à ne communiquer *que* l'identité du responsable du traitement et la finalité, si et seulement si, le projet de traitement présente tous les éléments de sécurisation que la Commission exige. Il est important de souligner que l'anonymisation à bref délai, lorsqu'elle présente toutes les conditions de sécurité, ne prive pas la CNIL de son pouvoir de contrôle de la pertinence des données traitées ni de son appréciation de l'opportunité du traitement.

205. Traitements ayant pour objet la prévention, la recherche et la constatation d'infractions pénales.- En l'espèce, la CNIL effectue un contrôle sur la pertinence des données traitées et les raisons justifiant une dérogation à l'obligation d'information en faisant une application stricte de l'article 32 VI de la loi «Informatique et Libertés». C'est-à-dire qu'elle contrôle qu'il s'agit bien d'un traitement ayant un objectif de prévention et non qui servait à prendre une décision pouvant avoir un impact sur la personne concernée. Elle s'assure également que le traitement se cantonne à la recherche et la constatation d'infractions pénales. La CNIL effectue donc un contrôle du traitement en vérifiant qu'il entre bien dans la qualification visée à l'article 26 I, 1°) et 2°)[713] de la loi «Informatique et Libertés» modifiée. La CNIL valide régulièrement les traitements qui sont effectués pour le compte de l'Etat, et, lorsqu'ils sont effectués dans un but de recherche et de prévention

[712] Ibidem note précédente.
[713] « Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'Informatique et des Libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;
2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. »

des infractions pénales. Elle accepte l'absence d'information de la personne concernée par le traitement[714].

Néanmoins, la CNIL peut se montrer plus exigeante et estimer que la dérogation à l'obligation d'information ne s'applique pas en cas de fichage de la personne, et ce, d'autant plus lorsque la personne avait connaissance de ce fichage. La CNIL a estimé que, compte tenu du fait que la personne avait connaissance du fichage au sein du « fichier judiciaire automatisé des auteurs d'infractions sexuelles ou violentes », il n'y avait pas de raison de ne pas informer la personne ainsi que les personnes destinataires des données[715]. La CNIL a également refusé que soit mis en place le traitement AGRASC pour la gestion et le recouvrement des biens saisis et confisqués par l'Agence de recouvrement des avoirs saisis et confisqués car la finalité du traitement ne correspondait pas la qualification de « prévention, de recherche et de constatation d'infractions pénales[716] ».

206. L'information préalable de la personne.- L'information préalable de la personne est visée à l'article 32 de la « LIL ». L'information préalable fait notamment référence aux mentions que le responsable doit communiquer à la personne concernée lors du traitement[717]. Il convient, ici, de rappeler que cette information doit être délivrée au moment où la collecte des informations est effectuée. Elle devra, entre autre, mentionner

---

[714] CNIL, délibération 2013-087, portant avis sur un projet d'arrêté relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé GARANCE (Gestion Automatisée de la Rédaction des Actes, des Notes et de la Circulation des Ecrits) - (Demande d'avis n° 1623908), du 28 mars 2013 ; Délibération n° 2012-084 du 22 mars 2012 portant avis sur un projet d'arrêté autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « Fichier national des objectifs en matière de stupéfiants » (FNOS) NOR: CNIX1231741X ; Délibération n°2012-061du 8 mars 2012 autorisant l'association HABEO à mettre en œuvre un traitement de données à caractère personnel ayant pour finalité la gestion et le suivi des situations de maltraitance envers les personnes âgées et les adultes handicapés via la mise en place d'une plateforme téléphonique de signalement, Autorisation n°1514929 ; Délibération n° 2011-418 du 15 décembre 2011 portant avis sur un projet de décret relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle, demande d'avis n° 1523917, JORF n°0108.

[715] CNIL, Délibération n° 2007-326, portant avis sur un projet de décret en Conseil d'Etat modifiant la partie réglementaire du code de procédure pénale et relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAIS) et au casier judiciaire national automatisé, du 8 novembre 2007.

[716] CNIL, Délibération n° 2011-344, portant avis sur un projet d'arrêté portant création d'un traitement automatisé dénommé « AGRASC » destiné à la gestion et au recouvrement des biens saisis et confisqués par l'Agence de gestion et de recouvrement des avoirs saisis et confisqués, du 10 novembre 2011.

[717] CF supra le principe de loyauté p147.

l'identité du responsable du traitement et les destinataires éventuels[718]. Ainsi, le site français « *Médisite* », concernant la possibilité de transmission des informations, indique de façon très générale que « ces informations peuvent être transmises aux sociétés du groupe X, par [son] intermédiaire, ces données peuvent être communiquées à des tiers. » L'utilisateur peut « ainsi être amené à recevoir des offres commerciales ou des propositions d'autres entreprises ou organismes ». Il possible de faire une comparaison avec les recommandations que la CNIL a pu faire dans son guide « La pub, si je veux » paru en 2011. La Commission indique ce que représente « dans les faits » une information *claire et lisible* :

« *Conformément à la loi «Informatique et Libertés» du 6 janvier 1978, ces informations sont nécessaires pour traiter votre demande. Elles sont enregistrées dans notre fichier de gestion de clientèle. Vous pouvez exercer votre droit d'accès et de rectification auprès de notre service clientèle. Si vous ne souhaitez pas que les données vous concernant soient transmises à nos partenaires cochez cette case* ».

La formulation, de l'AAI ci-dessus, est plus claire, en ce sens où il est possible de localiser le responsable du traitement. Elle reflète, d'un point de vue pratique, la possibilité d'exercer son droit de manière *directe* en cochant une « case ». On remarque, dans l'exemple de formulation de la CNIL, que l'information mentionne la possibilité d'exercer son droit d'opposition, droit que nous n'étudierons pas ici[719].

207. La conservation des données à des fins historiques, statistiques ou scientifiques.- Cette dérogation à l'obligation d'information est la cinquième exception visée par l'article 32 §III de la « LIL » de 1978. Cette exception vise la conservation et la réutilisation des données visées par le livre II du Code du patrimoine ainsi que l'obligation d'information, la coordination et le secret en matière de statistiques prévus à l'article 7 bis de la loi de 1951[720] qui prévoit les conditions dans lesquelles ces données peuvent faire l'objet d'une conservation et d'une réutilisation.

[718] Art 32 III de la « LIL » de 1978, op. cit. loci.
[719] Cf. infra p202.
[720] Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques.

Ainsi, dans l'hypothèse où les données doivent faire l'objet d'un archivage, l'article 36[721] de la « LIL » de 1978 prévoit la dispense de l'obligation d'information préalable de la personne concernée par le traitement. La dérogation prévue par l'article 32 §III de la « LIL » de 1978 s'applique, non seulement aux données issues de documents publics qui sont archivés, mais, elle s'applique également à la réutilisation de ces dernières. Cependant, la dérogation à l'obligation d'informer la personne concernée par ces traitements ne s'applique qu'à l'obligation d'informer la personne de façon individuelle[722]. En effet, la CNIL affirme que, dans le cas de la réutilisation des données à caractère personnel, la réutilisation de ces données ou leur diffusion en ligne doivent faire l'objet d'une nouvelle information générale « claire et précise [723]».

Enfin, l'article 7 bis de la loi de 1951 prévoit la situation où l'administration souhaite transmettre les données à l'INSEE afin que soient établis des statistiques, exception prévue par l'article 32 §III de la « LIL » qui autorise la transmission des données sans avertir individuellement les personnes concernées. La CNIL adopte la même position en la matière mais insiste cependant sur le fait qu'une information générale doit être renouvelée[724].

---

[721] « Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine. Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives dans le cadre du livre II du même code sont dispensés des formalités préalables à la mise en œuvre des traitements prévues au chapitre IV de la présente loi. Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa : soit avec l'accord exprès de la personne concernée ; soit avec l'autorisation de la Commission nationale de l'informatique et des libertés ; soit dans les conditions prévues au 8° du II et au IV de l'article 8 s'agissant de données mentionnées au I de ce même article. »

[722]CNIL, délibération n° 2010-460 du 9 décembre 2010 portant recommandation relative aux conditions de réutilisation des données à caractère personnel contenues dans des documents d'archives publiques. JORF n°0026 du 1 février 2011. Voir aussi délibération n°2012-113 du 12 avril 2012 portant autorisation unique de traitements de données à caractère personnel contenues dans des informations publiques aux fins de communication et de publication par les services d'archives publiques (décision d'autorisation unique AU-029).

[723] *Ibidem*

[724] CNIL, délibération n°2013-105, autorisant l'Institut National des Etudes Démographiques (INED) à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la réalisation et l'analyse des résultats de l'enquête téléphonique réalisée auprès des parents des enfants âgés de deux ans inclus dans la cohorte « Elfe », du 25 avril 2013 ; Voir aussi la Norme Simplifiée n°26, concernant les traitements automatisés à caractère statistique effectués, à partir de documents ou de fichiers de gestion contenant des informations nominatives sur des personnes physiques, par les services producteurs d'informations statistiques au sens du décret n 84-628 du 17 juillet 1984, *in* Arrêté du 12 décembre 2008 relatif au traitement automatisé de l'enquête statistique « bâtiments d'élevage ».

Il semble que la dérogation à l'obligation d'information dans le cadre de la conservation des données à des fins historiques, statistiques ou scientifiques ne soit pas une dérogation totale à l'obligation d'informer. En effet, la CNIL applique, en la matière, une analyse au cas par cas et n'autorise le défaut d'information individuelle que lorsqu'une information générale est respectée par le responsable du traitement.

La Commission se montre très stricte en matière d'information et accepte, seulement dans certains cas, que l'obligation d'information soit contournée, ceci, même lorsque le responsable du traitement juge que l'accomplissement de cette obligation est impossible ou demande des « efforts disproportionnés » compte tenu de la finalité du traitement.

208. L'information impossible ou demandant des efforts disproportionnés par rapport à la finalité du traitement.- Cette dérogation trouve sa raison d'être dans l'hypothèse d'un traitement indirect de données à caractère personnel. C'est-à-dire que le responsable du traitement fonde sa demande sur la finalité du traitement qui n'a aucune relation avec les données traitées[725]. Ce fondement est souvent invoqué compte tenu du grand nombre d'informations contenues dans les fichiers mais qui ne sont pas prises en compte lors du traitement. Ce fondement est accepté par la Commission lorsque les traitements qui sont envisagés tendent à l'amélioration des moyens d'action de l'administration, l'informatisation des bases de données ou la transmission d'actes[726]. De même, la CNIL accepte une *diminution* de l'obligation d'information pour les prestataires qui effectuent un traitement automatisé sur le territoire français, pour le compte d'un

[725] CNIL, délibération n°2012-245, autorisant la Cour de Cassation, à mettre en œuvre un traitement de données à caractère personnel ayant pour finalité la constitution de base de jurisprudence Jurinet, du 19 juillet 2012.

[726] CNIL, délibération n°2011-423 autorisant la société *Geolsementics* à mettre en œuvre à titre expérimental, dans le cadre du projet de recherche, les traitements de données à caractère personnel nécessaires au développement d'un outil, dénommé SAIMSI, du 15 décembre 2011 ; délibération n°2006-056, concernant la dispense de déclaration des traitements mis en œuvre par les collectivités territoriales et les services du représentant de l'Etat dans le cadre de la dématérialisation du contrôle de légalité du 2 mars 2006 ; délibération n°2010-117, portant avis sur le projet d'arrêté autorisant la mise en œuvre d'un traitement automatisés de données à caractère personnel dénommé « Gestion des amendes forfaitaires des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées » du 6 mai 2006, délibération n°2013-013, autorisant l'INAVEM à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité le suivi des activités des associations d'aide aux victimes adhérentes et l'établissement de statistiques, du 24 janvier 2013.

responsable de traitement établi hors de l'UE et pour des informations collectées hors de l'UE. Cette autorisation a été motivée par des raisons d'opportunités contractuelles[727] :

« Le transfert est en effet considéré comme nécessaire :

- à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ; ou

- à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers. »

209. Le refus de la qualification *d'information impossible* ou d'*efforts disproportionnés*.- La raison principale invoquée par le responsable du traitement est que, lorsqu'il s'agit de collectes indirectes de données, il est parfois difficile de *toucher* la personne concernée par le traitement afin de l'informer des données qui sont collectées à son sujet. La Commission analyse de façon stricte les conditions de l'impossibilité d'informer la personne. En effet, dans la délibération n°2011-124 du 5 mai 2011, la Commission rejette les motivations du Ministère de la santé qui invoque le caractère disproportionné que nécessite l'information des personnes figurant comme « personnes à prévenir » lors de la mise en place d'un traitement permettant à des personnes âgées de se référencer dans un répertoire leur faisant bénéficier d'une assistance en cas d'accident[728].

En matière de collecte sur le réseau internet, la CNIL se montre plus sévère vis-à-vis des moteurs de recherche. En effet, la Commission a rejeté l'argumentation de la société *Directannonces* qui avait collecté des données de particuliers via des annonces immobilières pour les transmettre à ses agents[729].

---

[727] Délibération n°2011-023 dispensant des traitements automatisés effectués sur le territoire français par des prestataires agissant pour le compte de responsables de traitement établis hors de l'Union européenne et concernant des données personnelles collectées hors de l'Union européenne. (DI-015), du 20 janvier 2011.

[728] CNIL, délibération n°2011-124, portant avis sur un projet d'arrêté autorisant les traitements de données personnelles dénommés Répertoires Locaux pour les Opérations de Protection des Personnes Agées, du 5 mai 2011, en l'espèce la Commission reste *fidèle* à sa position en matière de traitements qui concernent directement les personnes, et, si elle rejette le caractère disproportionné invoqué par le ministère, elle ne considère pas le traitement illicite, mais affirme qu'il est au moins nécessaire d'informer les « personnes à prévenir » de l'existence de ce traitement.

[729] CNIL, délibération n°2009-148, prononçant une sanction pécuniaire à l'encontre de la société *Directannonces,* du 26 février 2009. En l'espèce, la société invoquait la difficulté d'informer les personnes dont les données avaient été collectées via un moteur de recherche. Voir aussi, Conseil d'Etat, 5 septembre 2008, n°319071.

Dans le cadre de l'information des personnes dont les données ont été collectées via les réseaux sociaux, la Commission a considéré que la société *Pages Jaunes* ne pouvait pas déroger à son obligation d'information en invoquant l'impossibilité de délivrer l'information[730]. En l'espèce, la société *Pages Jaunes* avait effectué une collecte d'informations issues de l'agrégation[731] des données communiquées par les réseaux sociaux. La Commission a donc considéré la collecte comme étant déloyale au sens de l'article 35 de la « LIL »[732]. Le Conseil d'Etat[733] a validé ce raisonnement[734] le 12 mars 2014 dans l'affaire *Google Street View.* En l'espèce, il était reproché à la société *Google* d'avoir effectué la collecte massive « d'identifiants Wifi » sans que les titulaires de ces réseaux n'en aient été informés. La société avait invoqué l'impossibilité d'informer chaque titulaire de routeur Wifi. La Commission a rejeté cette argumentation au motif qu'il n'était, certes, pas possible d'effectuer une information individuelle, mais qu'une information générale était de rigueur compte tenu de l'opération massive de collecte de données.

210. Les sanctions en cas d'absence d'information.- Dans la plupart des hypothèses la CNIL se trouve dans une situation où le responsable du traitement a été, soit négligeant, soit a sciemment fait preuve de mauvaise volonté concernant son obligation d'information. Dans la majeure partie des affaires, la CNIL effectue une mise en demeure avant de prononcer une sanction. Pour l'année 2015, 93 mises en demeure ont été adoptées par la Commission alors que dix sanctions ont été prononcées[735]. Néanmoins, la CNIL semble adopter des sanctions adaptées à la structure qui a commis un manquement. En effet la Commission a prononcé une sanction pécuniaire de 10 000 Euros à l'encontre de la société *SAS Professional Consulting,* car elle avait mis en place un système de vidéosurveillance qui n'avait pas été porté à la connaissance des salariés[736]. La Commission peut se montrer compréhensive vis-à-vis des difficultés de mise en œuvre de l'obligation d'information, notamment en raison du coût élevée que celle-ci peut entrainer. La Commission n'a pas

[730] CNIL, délibération n°2011-203, portant avertissement à l'encontre de la société *Pages jaunes,* du 21 septembre 2011.
[731] *Ibidem.*
[732] *Ibidem.*
[733] Conseil d'Etat, 12 mars 2014, n°353193, mentionné au recueil Lebon.
[734] CNIL, délibération n° 2011-035, prononçant une sanction pécuniaire à l'encontre de la société *Google Inc.,* du 17 mars 2011.
[735] CNIL, Bilan d'activité annuel 2015, publié le 8 avril 2016.
[736] CNIL, délibération n°2013-139, prononçant une sanction pécuniaire à l'encontre de la société *PS Consulting,* du 30 mai 2013. Précisons que dans cette affaire, la CNIL a relevé aussi le fait que le système mis en place par l'entreprise ne présentait pas un niveau de sécurité suffisant.

retenu l'intention du responsable du traitement de se soustraire à son obligation mais a prononcé une sanction pécuniaire de 100 000 euros[737] à l'encontre de la société *Google Inc.* qui avait les moyens de mettre en place une information générale.

Les bilans effectués par la Commission démontrent que, dans la plupart des cas, les manquements soulevés ont été régularisés après mise en demeure[738].

211. Sanctions en cas d'information incomplète ou *partielle.-* Comme envisagé dans la partie 1, il appartient au responsable du traitement de mettre en œuvre tous les moyens pour informer la personne du traitement de ses données. Il doit également apporter la preuve[739] que cette information a bien été communiquée. La Commission exige que les conditions visées à l'article 32 §I de la « LIL » soit remplies ; de fait la CNIL considère que l'information est insuffisante lorsque, dans le cadre d'une surveillance vidéo, l'affichage du seul panneau « vidéo » n'est pas une information complète[740]. En matière de communication, la Commission ne considère pas comme une information complète[741] la seule mention « stop » dans un SMS au motif que, celle-ci n'est pas une information suffisante concernant le « droit d'opposition »[742]. En ce qui concerne l'obligation d'information sur les réseaux sociaux, la CNIL a publiquement mis en demeure[743] la société *Facebook Inc.* aux motifs que la société ne délivre « aucune information […] aux internautes sur leurs droits et sur l'utilisation qui sera faite de leurs données sur le formulaire d'inscription au service » et que la société collecte de façon massive des informations à leur insu.

---

[737] CNIL, délibération n°2011-035 op. cit. loci. Dans laquelle la Commission prononce une sanction pécuniaire de 100 000 euros à l'encontre de la société *Google Inc.*

[738] La nouvelle possibilité d'action « en ligne » de la CNIL lui permet de dispenser ses recommandations aux sites de manière plus rapide. 501 contrôles ont été effectués par la Commission. Bilan annuel d'activité 2015, 36ème rapport disponible sur www.cnil.fr.

[739] CNIL, délibération n° 2012-209 du 21 juin 2012 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects (Norme simplifiée n° 48)

[740] CNIL, délibération n°2010-112, décidant de l'interruption d'un traitement vidéo, du 22 avril, 2010 ; délibération n°2009-201, prononçant une sanction pécuniaire de 10 000 Euros à l'encontre de la société *JM Philippe,* du 16 avril 2009.

[741] Conseil d'Etat, 23 mars 2015, n°357556, mentionné aux Tables du recueil Lebon.

[742] CNIL, délibération n°2011-384, prononçant une sanction pécuniaire de 20 000 Euros à l'encontre de la société Groupe *DES France,* du 12 janvier 2012.

[743] CNIL, décision n° 2016-007, mettant en demeure les sociétés *Facebook Inc. et Facebook Ireland,* du 26 janvier 2016 ; délibération n°2016-026, du bureau de la CNIL décidant de rendre publique la mise en demeure n°2016-026, du 4 février 2016.

La Commission se montre exigeante en ce qui concerne l'obligation d'information et considère que si l'information ne peut pas se faire de façon individuelle elle doit se faire, pour le moins, de façon générale et de manière à ce que les personnes concernées par le traitement puissent accéder à leurs informations et exercer leur droit d'accès et de rectification.

Section 2 : Le droit d'accès et le droit d'opposition au traitement des données

Le droit d'accès est un droit essentiel car il permet à la personne d'avoir connaissance du contenu réel des informations la concernant. Le droit d'accès est un droit à *double détente* en ce sens où il regroupe, en réalité, le droit de rectification (a) et le droit d'opposition (b).

a) Le droit d'accès, de rectification et d'effacement

212. Contenu.- Le droit d'accès et de rectification est prévu tant par la directive 95/46/CE de 1995 que par loi «Informatique et Libertés» de 1978. Les articles 90 et suivants du décret du 20 octobre 2005 complètent les garanties du droit d'accès et de rectification. Dans le cas où le responsable du traitement refuserait l'accès aux informations, le Code pénal prévoit une sanction aux articles R625-11 et 625-12 d'une contravention de cinquième classe.

L'article 39 de la Loi «Informatique et Libertés» dispose que :

> *I.-Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :*
>
> *1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;*

2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;

4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle.

Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition.

213. L'attrait du droit d'accès est qu'il ne doit pas faire l'objet d'un intérêt à agir[744]. Le droit d'accès, comme les autres droits reconnus aux personnes concernées par un traitement de données, est un droit individuel. En conséquence, selon la CNIL, « s'agissant d'un droit strictement personnel, celui-ci ne peut être exercé que par son titulaire et le mandat ne peut être utilisé, selon les règles du droit commun, que pour les mineurs et incapables majeurs »[745].

214. La portée du droit d'accès et de rectification.- L'autre intérêt de ce droit est qu'il renverse la charge de la preuve. En effet, l'article 36[746] de la « LIL » prévoit qu'il appartient au responsable du traitement d'apporter la preuve que les données sont exactes et qu'elles devaient faire l'objet du traitement. Dans le cas où les données ont été collectées

[744] CNIL, Délibération n° 80-10 du 1er avril 1980 portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés.
[745] *Ibidem*.
[746] Article 36 de la « LIL » dans son ancienne rédaction op.cit.loci.

directement auprès de la personne à qui il appartient de délivrer des informations exactes, le responsable du traitement devra apporter la preuve que la personne a donné son consentement de façon exprès. Il convient également de souligner que la réforme de la loi «Informatique et Libertés» de 2004 apporte la possibilité à la personne concernée de « verrouiller » ses données. C'est-à-dire que la personne concernée peut demander au responsable du traitement de refuser l'accès des données à certaines personnes ou prestataires. Une fois que la personne a fait une demande de rectification, l'article 40 alinéa 3 de la « LIL » prévoit que le responsable du traitement doit apporter la justification, « sans frais pour le demandeur », qu'il a effectué l'opération de rectification visée à l'alinéa 2[747]. L'alinéa 4 de l'article 40 de la « LIL » ajoute que la personne concernée a ainsi droit d'obtenir le remboursement des frais engagés pour le coût de reproduction des données. La CNIL insiste, là encore, sur le fondement de l'article 39 §I, 1°) de la Loi «Informatique et Libertés» en disant que, les données délivrées doivent être produites sous une forme « accessible [748]», c'est-à-dire sur un support matériel qui permette de les consulter facilement. Elles doivent également être intelligibles[749] de sorte qu'elles puissent faire transparaître l'intention du responsable du traitement de mettre la personne concernée en position d'exercer son droit d'accès et de rectification.

Lors de la transposition de la directive de 1995, la loi du 6 août 2004 a repris la disposition de l'article 12 a) de la directive 95/46/CE et a inclu la possibilité, pour la personne concernée, d'avoir accès à l'origine des données[750]. Cette disposition se justifie dans un contexte où les données sont collectées et agrégées auprès de nombreux intervenants, ce qui entraîne la possibilité de pluralité de significations des données traitées. L'accès aux données *originelles* permet en cas d'erreur ou de communication non consentie, à un tiers d'identifier le responsable du traitement d'origine.

215. L'accès à la signification déduite des données.- Cette prérogative est visée par l'article 39 §I, 5°) de la loi «Informatique et Libertés» modifiée. La signification des

[747] Article 40 de la « LIL » op.cit.loci.
[748] CNIL, délibération n°2012-213 portant une sanction pécuniaire à l'encontre de la société *Equipements Nord Picardie,* du 22 juin 2012. Voir aussi l'article 95 du décret du 20 octobre 2005 qui prévoit qu'un lexique permettant d'expliquer les termes et abréviations. Décret n°2005-1309 op. cit. loci.
[749] Cass. Crim. 6 mai 2008, *SFR Cegetel,* n°07-82.2000, Comm. Com. électr., 2008, n°117, note A. Lepage.
[750] Article 34 et 34*Bis* de la « LIL » modifiée op. cit. loci.

données traitées est formulée sous la forme de « logique qui sous-tend le traitement automatisé ». Le législateur français ne prévoit cette possibilité que lorsque ces données ont fait l'objet d'une prise de décision produisant des effets juridiques ou une décision prise sur la base des données traitées. Cette disposition est d'autant plus importante dans le contexte de l'*Open Data* et du *Data Meaning.* En effet, dans un contexte où les données font l'objet de nouveaux traitements grâce à l'utilisation des algorithmes, notamment par les éditeurs de logiciels et d'applications, le droit d'accès à ces informations est une prérogative dont l'usage est essentiel pour rendre le droit de rectification efficace. Les données dont la « logique […] sous-tend le traitement automatisé » concernent également les traces (*logs)* que laisse la personne lorsqu'elle consulte ou effectue des opérations sur internet. Ces traces sont des données à caractère personnel dès lors qu'elles permettent d'identifier une personne directement ou indirectement. Dès que les logs émanent du compte de l'utilisateur, ces fichiers doivent êtres qualifiés de données à caractère personnel[751]. La Commission considère également que les données ayant fait l'objet d'un traitement par le biais de logiciels de calculs, de raisonnements programmés[752] ou de statistiques[753] permettant de cibler un comportement, doivent pouvoir faire l'objet d'un droit d'accès sans que puissent être opposés, à la personne concernée par le traitement, ni le secret des affaires, ni l'intérêt économique et industriel du responsable du traitement[754].

Néanmoins, la CJUE a considéré récemment que l'exercice du droit d'accès devait être limité dans le cas d'une décision de justice contenant « une analyse juridique ». La Cour affirme que ces informations ne peuvent pas être qualifiées de données à caractère personnel, même lorsque cette « analyse juridique » contient des données telles que le nom, l'âge ou la nationalité[755]. En l'espèce, il s'agissait de savoir si les analyses juridiques contenues dans les décisions individuelles relatives au droit de séjour devaient être considérées comme des données à caractère personnel. Ainsi, le juge européen a indiqué, dans son analyse, de la directive européenne 95/46/CE du 24 octobre 1995 que, le droit d'accès contenu dans ladite directive avait pour vocation la vérification de l'exactitude des

[751] CNIL, délibération n° 2016-005, portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les organismes publics et privés pour la préparation, l'exercice et le suivi de leurs contentieux ainsi que l'exécution des décisions rendues (AU-046) du 14 janvier 2016.
[752] Cf supra les nouveaux gisements de données.
[753] Cf les scores de clients mauvais payeurs.
[754] Cnil, délibération n°92-032 relative au contrôle effectué le 2 octobre 1992 à la Caisse Régionale de Crédit Agricole de Dordogne, du 6 avril 1993.
[755] CJUE, 17 juillet 2014, affaires jointes C-141/12 et C-372/12, YS contre Minister voor Immigratie, Integratie en Asiel et Minister voor Imigratie, Integratie contre M.S.

données et de la licéité du traitement, alors qu'en l'espèce, les requérants faisaient une simple demande d'accès aux documents et, par conséquent, la directive 95/46/CE n'avait pas vocation à s'appliquer[756].

216. Les limites du droit d'accès et de rectification.- L'article 39 §II de la loi «Informatique et Libertés» prévoit que le responsable du traitement peut refuser, pour des raisons légitimes, l'accès aux informations. Dans sa recommandation, la CNIL[757] indique qu'il appartient au responsable du traitement de rapporter le caractère abusif, répété ou imprécis de la demande. Dans le cadre des données archivées, l'article 39 §II prévoit que le responsable du traitement peut s'opposer à l'accès si : le mode de conservation et la nature des données excluent tout risque d'atteinte à la vie privée et que la durée de conservation des données n'excède pas celle nécessaire à l'établissement de statistiques ou de recherches scientifiques ou historiques. De même, lorsque les données font l'objet d'un archivage définitif, la Commission indique que, pour en refuser l'accès, il doit apporter la preuve que les moyens techniques d'archivage sont de nature à ne pas porter atteinte à la vie privée[758].

217. L'accès au Dossier Médical Partagé.- Le décret d'application de la loi de modernisation de notre système de santé du 26 janvier 2016 prévoit que le titulaire du Dossier Médical Partagé peut exercer son droit d'accès, conformément à l'article 40 de la loi «Informatique et Libertés». L'alinéa 3 de l'article R. 1111-37 du Code de la santé publique prévoit que le titulaire ne peut supprimer les données reportées par un professionnel de santé qu'en invoquant un motif légitime[759] auprès du professionnel qui en est l'auteur[760]. Pour garantir au titulaire la maîtrise de son dossier, le législateur doit

---

[756] Ibid. CJUE, 17 juillet 2014 ; Voir aussi*, « Interprétation classique de la directive relative au traitement des données personnelles et approche restrictive du champ d'application de l'article 41, paragraphe 2, de la Charte des droits fondamentaux »,* Protection des données personnelles, J. Dupont-Lassalle, Europe n°10, Octobre 2014, comm. 368.

[757] CNIL, Délibération n° 80-10 du 1er avril 1980 op. cit. loci.

[758] Concernant les moyens de preuves le responsable du traitement doit être en mesure de rapporter les moyens de sécurité comme les méthodes de « chiffrement des données ». CNIL, délibération n°2005-213 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.

[759] Cf droit d'opposition.

[760] Décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé, JORF n°0155 du 5 juillet 2016.

prendre en compte le fait que les données sont souvent disséminées entre les divers intervenants, ce qui constitue une difficulté supplémentaire pour accéder aux informations.

218. L'interopérabilité des réseaux, une nécessité.- La Commission européenne, dans sa recommandation du 2 juillet 2008, a défini l'interopérabilité des systèmes des dossiers de santé comme « la capacité de plusieurs systèmes de dossiers informatisés de santé d'échanger aussi bien des données exploitables par un ordinateur que des informations et des connaissances demandant une intervention humaine ». En pratique, les conventions d'interopérabilité conduisent à des protocoles que chaque concepteur doit respecter. Les éditeurs de produits de sécurité et les prestataires de services de confiance sont également visés par ces conventions, dans la mesure où ils doivent proposer aux autorités administratives des produits et des prestations conformes aux exigences du Référentiel Général de Sécurité[761].

Les référentiels d'interopérabilité et de sécurité sont visés par l'article L.1110-4-1[762] du Code de la santé publique qui définit les mesures de sécurisation physique et logique, les modalités d'accès et de traitement, les mesures d'identification et d'habilitation, les procédures de traçabilité, les historiques concernant les accès aux informations et les mesures mises en œuvre pour garantir la confidentialité dont le chiffrement de tout ou partie des informations recueillies. L'enjeu de l'interopérabilité est de rendre la communication compréhensible à travers un ensemble de conventions techniques que l'on peut qualifier de « système formel ». L'autre aspect de cette nécessité est de permettre une interopérabilité des systèmes et de garantir une communication *exhaustive* des informations car les données peuvent être contenues sur divers supports. Cette situation se traduit, en pratique, par le fait que certaines informations peuvent être détenues par un sous-traitant ou se trouver dans une messagerie ou des dispositifs nomades comme les terminaux portables (ordinateurs, clefs USB etc.) voire répartis dans des services différents. Ainsi, le responsable du traitement[763] doit être en mesure de répondre à la

[761] L'article 9 de l'ordonnance n°2005-1516 du 8 décembre 2005[761] a créé les Référentiels Généraux de Sécurité (RGS) afin de parvenir à une coordination des moyens de communiquer par voie électronique. Dans le cadre de cette étude, les RGS sont déclinés avec le Référentiel Général d'Interopérabilité (RGI).
[762] Modifié par le décret du 4 juillet 2016 op. cit. loci.
[763] La Caisse Nationale d'Assurance Maladie et Travailleurs Salariés (CNAMTS) en l'occurrence, désignée par l'article R. 1111-27 CSP. Voir aussi : CNIL, délibération n°2016-147 portant avis sur un projet de décret en Conseil d'Etat au dossier médical partagé, demande d'avis 16010151, du 12 mai 2016.

demande d'accès de la personne concernée par le traitement. Il doit donc veiller à ce que l'organisation des données puisse permettre une communication complète des informations.

219. Le rôle efficace des « traces ».- Le rôle des traces (logs) a été fortement défendu dans le rapport « Fagniez[764] ». En effet, les traces des différents intervenants ayant agi[765] ou ayant consulté le DMP du titulaire constituent la garantie de l'exercice de prérogatives comme la suppression ou la rectification de données. Ces « fichiers logs » sont des éléments de preuve concernant le droit « de masquage », autrement dit, le droit d'opposition. Dans son guide destiné aux professionnels de santé, la Commission insiste sur la capacité des intervenants à permettre à l'utilisateur de s'informer. Cette capacité passe, non seulement par des moyens sécurisés de conservation, mais, également, par la durée de conservation[766]. A l'origine, la Commission se contentait d'indiquer que la conservation des données et des traces ne devait pas être illimitée. Le décret d'application n°2016-914[767] a fixé le délai de conservation des données et des traces à 10 ans. Ce délai correspond au délai de prescription de l'action en responsabilité médicale[768]. Certains auteurs[769] pourront se féliciter d'avoir anticipé la nécessité de mettre en place un texte prévoyant une conservation « décennale » en matière de données de santé à caractère personnel permettant ainsi d'assurer l'effectivité du droit d'accès et « de masquage ».

220. Le droit d'accès aux fichiers de police judiciaire.- Ce type de traitement est spécifique au sens où, « par dérogation aux articles 39 et 40 [de la loi «Informatique et Libertés»], lorsqu'un traitement intéresse la sureté de l'Etat, la défense ou la sécurité

---

[764] Rapport au ministre de la santé et des solidarités, Le masquage d'informations par le patient dans son DMP, P-L. Fagniez, 30 janvier 2007, La Doc. Fr. 2008, *Coll.* Rapport Public.
[765] L'utilisation de la Carte Professionnel de Santé (CPS) est régie par l'article L.161-33 alinéa 4 du Code de la sécurité sociale. Ce dernier stipule que la CPS est utilisée pour l'ouverture de droits aux prestations de l'assurance maladie pour l'un de ses bénéficiaires. Cette carte est aussi utilisée par les médecins pour établir les certificats de décès par voie électronique, après s'être authentifié, comme en dispose l'article R. 2213-1-2 du Code général des collectivités territoriale. L'authentification par la CPS offre des garanties agréées par le groupement d'intérêt public mentionné à l'article R.161-54 du Code de la sécurité sociale. Les données du volet médical sont, elles, transmises par le médecin, après chiffrement, à l'Institut National de la Santé et de la Recherche Médicale ou à l'organisme chargé par cet institut de gérer le système de collecte et de transmission des certificats saisis.
[766] CNIL, Guide professionnel de santé, édition 2011.
[767] Décret du 4 juillet 2016 op. cit. loci.
[768] Article L1111-18 CSP.
[769] C. Zorn-Macrez, « Données de santé et secret partagé » op. cit. loci. Page 353.

publique [770]», le droit d'accès aux informations devra se faire de façon indirecte. Ce type de traitement fait référence aux fichiers STIC, JDEX et TAJ[771]. Ce type de traitement est prévu par l'article 26 de la « LIL » qui autorise, après décret pris en conseil d'Etat et avis de la CNIL, le traitement d'informations relatives aux antécédents judicaires d'une personne. Ce type de traitement automatisé est prévu par la loi n°2011-267 du 14 mars 2011 dite loi *LOPPSI II*[772]dont les dispositions sont visées aux articles 230-6 et 230-11 du Code de procédure pénale.

221. L'Etat, responsable du traitement.- C'est le Procureur de la République qui est désigné pour effectuer le traitement des données et qui est habilité à demander que les données soient modifiées ou effacées, notamment lorsque la personne concernée est relaxée. Il a pour *mission* d'informer le gestionnaire des fichiers des décisions de non-lieu. En pratique, cette demande se traduit par une mention interdisant la consultation des fiches rectifiées lors des enquêtes administratives. En matière d'effacement, la France s'est vue condamnée par la Cour Européenne des Droits de l'Homme (CEDH) dans l'arrêt *Brunet contre France*[773], dans lequel la Cour Européenne indique que le procureur n'est pas mis en position d'effectuer l'effacement.

Enfin, concernant la durée de conservation, l'article 230-11 du Code de procédure pénale prévoit un tableau de durée de conservation selon l'infraction commise en fonction de l'âge de la personne.

Comme le constate régulièrement la CNIL dans ses rapports d'activité[774], les principales demandes d'accès à ce type de fichiers proviennent de personnes qui se sont vu refuser un emploi. La Commission regrette d'avoir à effectuer autant de constats de dysfonctionnements des fichiers. Elle regrette notamment que le droit de mise à jour visé à l'article 6, 4°) de loi «Informatique et Libertés» ne soit pas appliqué de façon plus stricte, ceci en raison de l'absence de réponse du Procureur auteur de l'inscription[775].

---

[770] Article 41 de la LIL de 1978 op. cit. loci.
[771] Respectivement : « Système de Traitement des Infractions Constatées » ; « système JUdiciaire de Documentation et d'EXploitation » ; « Traitement Antécédent Judiciaire » qui regroupent les fichiers de police et de gendarmerie.
[772] Loi d'Orientation et de Programmation pour la Performance de le Sécurité Intérieure.
[773] CEDH, 18 septembre 2014, affaire n°2010/10, *Brunet contre France*.
[774] Voir la conférence de presse du 16 mai 2008 lors de la présentation de son 28ième rapport d'activité 2007 page 5 et s. ; Rapports d'activité annuels 2004 à 2011, La Doc. Fr. coll. Rapports officiels.
[775] Ibidem note précédente.

Quoi qu'il en soit, le droit d'accès et de rectification ne peut s'exercer que lorsque le traitement est déjà mis en œuvre et lorsque la personne souhaite avoir la maîtrise de ses données. Au-delà de ces droits, la personne peut souhaiter mettre un terme au traitement. Elle peut grâce à son droit d'opposition qui est un droit qui s'exprime, en principe, lorsque le traitement est déjà mis en œuvre. Néanmoins, on peut se poser la question de savoir si ce droit n'est pas le prolongement de l'expression du consentement de la personne à ce que ses données fassent l'objet d'un traitement. Or, le consentement doit être recueilli en amont du traitement, et, par déduction, on peut conclure que le fait de consentir est, aussi, le droit de ne pas consentir. Si l'on se réfère à la rédaction originelle de la loi «Informatique et Libertés», le droit d'opposition existait avant même que le consentement ne soit pris en compte lors de sa réforme en 2004. Le droit d'opposition serait donc un droit *autonome* et rattaché à la personne. La CNIL indique que le droit d'opposition a une portée très large et a vocation à s'appliquer même lorsque les données n'ont pas été collectées directement auprès de la personne[776].

b) Le droit d'opposition

Le droit d'opposition est prévu par l'article 38 de la loi «Informatique et Libertés» modifiée.

> *« Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.*
>
> *Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.*
>
> *Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement. »*

222. L'exercice du droit d'opposition, droit commun.- Contrairement au droit d'accès et de rectification visé à l'article 40 de la « LIL » qui peut s'exercer sans motif légitime, le droit d'opposition ne peut s'exercer que lorsque la personne concernée par le

[776] CNIL, délibération n°2014-041, prononçant une sanction pécuniaire à l'encontre de l'association *Juricom & Associés,* du 29 janvier 2014.

traitement rapporte la preuve d'un motif légitime à ce que le traitement soit mis en œuvre. En d'autres termes, le motif légitime invoqué par la personne se caractérise par la preuve d'un intérêt particulier. Le considérant 45 de la directive européenne[777] fonde l'exercice du droit d'opposition de la personne sur « des raisons prépondérantes et légitimes tenant à sa situation particulière ». Par conséquent, les motifs légitimes feront l'objet d'une appréciation *in concreto*[778] c'est-à-dire au cas par cas.

223. L'appréciation du motif légitime.- L'exercice du droit d'opposition est un droit attaché à la personne et il ne peut être exercé que par le titulaire de ce droit. On peut, ici, faire une comparaison avec l'article 31[779] du Code de procédure civile qui dispose de deux conditions cumulatives pour que l'action en justice soit recevable : la qualité à agir et un intérêt légitime à agir. Néanmoins, en matière de protection de données à caractère personnel, l'intérêt à agir pour l'exercice du droit d'opposition n'est pas subordonné à l'existence d'un contentieux ou à la nécessité de « défendre une prétention ». En effet, la loi «Informatique et Libertés» prévoit que l'exercice du droit d'opposition peut être enclenché dans le cadre d'un traitement de données parfaitement légal. Par conséquent, la charge de la preuve est inversée, contrairement à l'exercice du droit d'accès et d'information. La Commission estime que l'appréciation du motif légitime, lorsqu'il fait appel à une situation « particulière [780]», relève de l'appréciation des tribunaux[781].

224. L'appréciation du motif légitime par le juge.- Les juridictions judiciaires ont souvent été saisies pour des demandes d'opposition au traitement restées sans réponse de la part du maître du traitement. Ces demandes sont souvent relatives à l'effacement de données publiées sur internet. Avant la réforme de la loi n°2004-801[782] du 6 août 2004 modifiant la « LIL » de 1978, la Cour de Cassation affirmait déjà que l'opposition des

[777] Directive européenne 95/46/CE op. cit. loci.
[778] CNIL, Délibération n°93-109 du 07 décembre 1993, relative à la demande d'avis de la CNAMTS concernant le traitement "IRIS", d'échanges d'informations par télétransmission entre organismes complémentaires et caisses primaires d'assurance maladie.
[779] « L'action est ouverte à tous ceux qui ont un intérêt légitime au succès ou au rejet d'une prétention, sous réserve des cas dans lesquels la loi attribue le droit d'agir aux seules personnes qu'elle qualifie pour élever ou combattre une prétention, ou pour défendre un intérêt déterminé. »
[780] Considérant 45 dir.Eur. 95/46/CE, Op. Cit. Loci.
[781] CNIL, délibération n°2012-404 portant recommandation relative aux traitements des données de consommation détaillées collectées par des compteurs communicants, du 15 novembre 2012.
[782] Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004, consacrant le droit d'opposition à l'article 38 alinéa 1 et 2.

abonnés à ce qu'ils soient sollicités dans le cadre de prospections commerciales était légitime lorsque l'opposition était fondée sur la protection de la vie privée[783]. De même, une personne dont le nom est diffusé sur internet dans l'objectif de faire un appel à témoins lors d'une révision de procès, constitue un motif légitime de retrait notamment en raison du caractère vexatoire et disproportionné de l'usage de ses données à caractère personnel[784]. En revanche, la Cour de Cassation, saisie de la question fondamentale de l'équilibre entre liberté de la presse et protection des données à caractère personnel, ne retient pas l'exercice du droit d'opposition contre la diffusion d'archives journalistiques en ligne, si ce droit n'est pas fondé sur l'inexactitude des faits[785]. Ainsi, la Cour exerce un véritable contrôle de proportionnalité lorsqu'il s'agit de questions fondamentales. En effet, dans l'arrêt du 28 septembre 2004, la Cour estime que le droit d'opposition est légitime dès lors qu'il est fondé sur la protection des opinions philosophiques, politiques ou religieuses[786]. Enfin, le Tribunal de Grande Instance de Paris considère que le motif légitime fondant le droit d'opposition doit s'apprécier au regard « de l'intérêt général du responsable du traitement » et les droits fondamentaux de la personne. Le TGI fonde sa décision sur l'article 7, 5°) de la « LIL » de 1978 et considère que le traitement est fondé sur l'intérêt légitime de l'organe de presse[787]. Les différentes décisions envisagées démontrent qu'il est difficile de retenir une définition préalable d'un motif légitime d'opposition au traitement et que l'appréciation doit se faire au cas par cas, grâce à l'intervention du juge. Néanmoins, la CNIL est aussi compétente pour apprécier le motif légitime.

225. L'appréciation du motif légitime par la CNIL.- La CNIL a été amenée, non pas à juger de la nature légitime du motif, mais à l'apprécier au travers des preuves rapportées par la personne concernée par le traitement. La Commission a estimé que le fait, pour des professionnels, de figurer sur un site permettant de les contacter au travers de l'utilisation d'un numéro surtaxé était un motif légitime d'opposition en raison du risque

[783] Cass. Crim. 29 juin 1999, n°97-84166, publié au bulletin, *JurisData* n°1999-003251.
[784] CA, Besançon 31 janvier 2007, n°RG 06/011896 ; D. 2007, observation A. Lepage ; voir aussi Cass. Crim., 20 février 2007, n°06-84310 publié au bulletin Crim n°51.
[785] Cass. 1re civ., 12 mai 2016, n° 15-17.729, M. Stéphane et Pascal X. c/ Les Échos : *JurisData* n° 2016-008910, com. N. Metallinos, Comm. Com. Electr. n° 7-8, Juillet 2016, comm. 64.
[786] Cass. Crim. 28 septembre 2004, n°03-86.604 publié au bulletin Crim. n°610.
[787] Dans cette affaire, le requérant souhaitait que ses informations concernant un viol dont il avait été relaxé soient retirées et que l'article de presse relatant cette affaire soit supprimé. Or, l'organe de presse qui avait publié l'article avait effectué une mise à jour de l'affaire avait indiqué que le prévenu avait été relaxé. TGI Paris, 23 mars 2015, Comm. Com. Electr. 2015, comm. N°45, obs. A. Debet.

d'atteinte à leur réputation[788]. De même, la Commission considère que la personne ne souhaitant plus figurer dans les registres d'une association est un motif légitime à ce que les informations[789] la concernant ne soient plus reliées à l'association.

Concernant le droit d'opposition du patient[790] à ce que certaines personnes aient accès à son dossier, la CNIL[791] estime que la personne (patient) qui s'oppose à ce que son dossier soit accessible par le système interne de l'établissement, au motif qu'un membre de sa famille est amené à travailler au sein de la structure, est un motif légitime d'opposition[792].

En matière d'utilisation de la biométrie en milieu scolaire, la Commission indique, dans sa délibération du 27 avril 2006, que le traitement de données à caractère personnel ayant pour support l'utilisation d'un dispositif de reconnaissance du contour de la main est autorisé lorsqu'un moyen alternatif est prévu en cas d'opposition au traitement. Elle insiste également sur le fait que la mise en place d'un tel dispositif « nécessite » une information individuelle des élèves majeurs ou de leurs représentants légaux[793]. En l'espèce, à la lecture de la délibération et de l'autorisation unique, il ressort que ce dispositif ne peut exister et être effectif que lorsque l'obligation d'information est dument respectée par le responsable du traitement. En effet, dans ce contexte, il semble que le droit d'opposition s'apparente à la possibilité de consentir ou de ne pas consentir au traitement. Or, on l'a vu, sur le fondement de l'article 8 de la « LIL » de 1978, l'information de la personne est la condition *sine qua non* de l'existence d'un consentement libre et éclairé en matière de traitement de données sensibles.

226. Le droit d'opposition au traitement des données de santé à caractère personnel.- Concernant la mise en place du Dossier Médical Partagé (anciennement Dossier Médical Personnel), la maîtrise des informations par le patient a suscité de vifs

[788] Il s'agissait, en l'espèce, de professionnels du droit dont les coordonnées avaient été collectées sur internet. CNIL, délibération n°2014-041, du 29 janvier 2014, op. cit. loci.
[789] En l'occurrence la personne souhaitait que son Curriculum Vitae soit retiré du site de l'association, CNIL, délibération n°2014-040 prononçant une sanction pécuniaire rendue publique à l'encontre de l'Association Société Française des Urbanistes, du 29 janvier 2014.
[790] Cf infra
[791] Ce droit d'opposition est aussi nommé « droit de masquage », terme employé dans le rapport « Fagniez » op. cit . loci.
[792] CNIL, Guide professionnel de santé, édition 2011, op. cit. loci.
[793] CNIL, délibération n°2066-103 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire, du 27 avril 2006, AU-009.

débats lors des discussions des droits donnés au patient. En effet, en 2007 le député P.L Fagniez affirmait que le droit conféré au patient de désigner ou d'exclure les personnes de l'accès à son dossier était capital, en ce sens où ce droit nommé « droit de masquage » était la « traduction » des articles 38 et 40 de loi « Informatique et Libertés ». Ce droit est aussi la traduction de l'article L.1110-4 du Code de la santé publique. A l'origine, la loi de 2004 prévoyait que, sauf dispositions expresses législatives ou règlementaires, le responsable du traitement était la personne, l'autorité publique, le service ou l'organisme qui était à l'origine du traitement. Il leur revenait l'obligation de déterminer la finalité du traitement. Par conséquent, il apparaissait que lorsqu'il s'agissait d'un dossier de réseau, c'était au réseau d'origine d'assurer la gestion et la sécurité du dossier numérique. Lorsqu'il s'agissait d'un organisme c'était à l'ASIP –Santé de gérer le dossier, notamment en ce qui concerne la mise en place de l'hébergement.

Le décret d'application n°2016-914 du 4 juillet 2016 de la loi de modernisation de notre système de santé dispose que la création du DMP est à l'initiative du titulaire ou du professionnel de santé. Le décret désigne la CNAMTS[794] comme responsable du traitement mais précise également que « ce dossier ne se substitue pas aux dossiers détenus par les établissements ». Cette dernière disposition peut paraître regrettable car elle ne contribue pas à ce que les informations soient centralisées sur un même support. Cette disposition peut également paraître contradictoire avec les nouvelles obligations qui pèsent sur les éditeurs de logiciels qui leur imposent de fournir des logiciels et applications intégrant des mécanismes d'interopérabilité[795]. Cette possibilité fait vraisemblablement écho au sentiment de défiance[796] éprouvé par les professionnels de santé à l'égard du droit de masquage. Le terme « masquage » n'est pas anodin en ce sens où, si l'on se réfère à la position de la CNIL concernant certains traitements, le droit de masquage fait référence à la protection du droit à la vie privée. Or, comme l'a affirmé la Commission dans le guide

[794] Art. R. 1111-27. La Caisse nationale de l'assurance maladie des travailleurs salariés est responsable de traitement au sens de l'article 3 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. « Elle s'assure de la conformité du dossier médical partagé l'article L. 1111-8 et aux référentiels d'interopérabilité et de sécurité mentionnés à l'article L. 1110-4-1.

[795] Référentiel de sécurité et d'interopérabilité.

[796] Un médecin s'opposant au droit au masquage déclare que les objectifs de transmission de données médicales de qualité du DMP ne pourront pas être remplis si les patients ont la possibilité de masquer des données de santé. Un médecin déclare qu'il serait incompréhensible que les patients puissent masquer des données à l'auteur de celles-ci. M. Chevillard, « *Le droit au masquage par le patient dans le cadre du Dossier Médical Personnel en France »,* Thèse en médecine 2007, page 48 et 49. Univ. Paris VI. N° 2007PA06G022.

« professionnel de santé » en 2011[797], la protection du droit à la vie privée constitue, à lui seu,l un motif légitime de s'opposer au traitement et à l'accès aux données concernant la personne. La position de la CNIL est partagée par le G29 qui indique que les responsables du traitement doivent, lors du traitement, prendre en compte l'impact[798] des données traitées sur la vie privée de la personne concernée par le traitement.

227. L'objectif de l'accès et de la maîtrise des informations directement par la titulaire s'explique par le fait que ce dernier doit pouvoir protéger et décider des éléments qui relèvent de sa vie privée. C'est-à-dire que la maîtrise des informations par le titulaire serait une manifestation concrète du « colloque singulier[799] » tant défendu dans le domaine de la santé. Cette possibilité doit cependant être envisagée avec la délivrance d'une information claire et précise du titulaire. Cette nécessité avait déjà été soulignée par le député P.L Fagniez dans son rapport de 2007. Il affirmait que le patient aurait ainsi la possibilité de tenir secrètes les informations au professionnel de santé, lui permettant de « se décider en conscience[800] ». Le titulaire du dossier peut, en effet, avoir la volonté de ne pas révéler des pathologies stigmatisantes particulièrement difficiles à vivre ; mais cette prérogative a souvent été considérée comme un risque d'aggravation du « risque de responsabilités médicales [801]» par les professionnels de santé. Certains[802] s'inquiètent de la « conséquence directe [de] l'individu [qui] acquiert une forme de légitimité, une capacité à opposer une « connaissance profane » au savoir médical historique. »

Il semble que Madame la Ministre de la santé M. Touraine ait pris en compte les craintes des professionnels de santé. En effet, l'article R. 1111-37 du Code de la santé publique prévoit, dans les mêmes conditions prévues par la « LIL[803] » de 1978, que le titulaire ne pourra s'opposer ou faire supprimer les données le concernant que lorsqu'il opposera un motif légitime[804] à l'auteur des données consignées. Néanmoins, le

---

[797] CNIL, Guide du professionnel de santé, éd. 2011, op. cit. loci.
[798] G29, Avis 05/2014 sur les Techniques d'anonymisation, adopté 10 avril 2014, WP216. Page 8 et 12.
[799] L'expression « colloque singulier », est attribuée à l'écrivain et médecin Georges Duhamel en 1935 lors de son discours d'investiture au CNOM.
[800] Rapport « Fagniez » op. cit. loci.
[801] Voir à ce sujet C. Zorn, « le droit à une pudeur verbale ? », *Colloque « la pudeur et le soin »,* Faculté de droit de Nancy, 28 mars 2008.
[802] Rapport CGEIET, « Bien Vivre grâce au numérique », R. Picard, février 2012 page 36.
[803] Article 40 de la loi n°78-17 op. cit. loci.
[804] Article R1111-37 du Code de la santé publique modifié par le décret 2016-914 op. cit. loci.

professionnel de santé devra concourir à une information complète et claire du titulaire, notamment en expliquant la finalité du DMP et le rôle des différents intervenants. Cette information doit en particulier indiquer au titulaire que le médecin traitant aura accès à l'ensemble des informations. Cet accès *permanent* du médecin traitant justifie, semble-t-il, le changement du caractère *Personnel* en *Partagé* car, dans le cadre de la nécessité de continuité[805] des soins, le médecin traitant sera admis à partager les informations dont il dispose à propos du patient avec une équipe médicale. On remarque, cependant, que le titulaire du dossier aura la capacité d'être le maître des informations qu'il aura lui-même consignées[806]. Dans le cadre de la gestion du DMP, le droit d'opposition ou de masquage s'apparente au retrait du consentement car l'assentiment de la personne concernant son dossier est l'élément déterminant pour que le dossier soit créé et maintenu[807]. La nouvelle loi de modernisation de 2016 semble permettre une plus grande maîtrise des données par le patient, mais la suppression ou l'opposition au traitement reste subordonnée à la preuve d'un motif légitime pour que l'exercice de ce droit soit efficace.

228. La nécessité d'une convergence harmonieuse entre le *médical* et la santé.- L'objectif de ce paragraphe est de traiter et de mettre en lumière le domaine de la santé au quotidien, c'est-à-dire sortir du cadre réglementaire médical pur. En effet, à l'ère de la société de l'information, les technologies permettant de « mieux vivre » au quotidien apparaissent dans le domaine de la santé et sortent du secteur « historique[808] » réglementé par la déontologie médicale. Cela nous mène à constater que les nouveaux acteurs industriels proposent des produits qui peuvent servir l'intérêt collectif. En effet, comme le constate R. Picard, les produits connectés qui apparaissent, dans un premier temps, comme des produits de consommation peuvent, dans un deuxième temps, devenir des outils qui peuvent agir positivement en matière de santé publique[809]. « Mais à un certain moment, il sera sans doute nécessaire de donner un cadre, des règles pour encadrer le développement

---

[805] Article L. 1110-1 CSP.
[806] R.1111-37 al 3 CSP modifié par décret 2016-941 op. cit. loci.
[807] Si le titulaire était mineur au moment de la création de son dossier médical partagé et sous réserve qu'il n'était pas émancipé, l'atteinte de l'âge de la majorité nécessite de recueillir son consentement pour conserver son dossier médical partagé. Il peut, à cette occasion, en demander la clôture. Article R. 1111-32 CSP modifié par le décret 2016-914 op cit loci.
[808] Il existe un risque « que se manifeste[nt] des tensions entre les opérateurs historiques et de nouveaux distributeurs », Rapport CGEIET page 26, op. cit. loci.
[809] Ibidem page 37.

de ce type de marché, pour apporter des garanties à l'utilisateur final. [810]». Ce constat permet également de prendre une position moins alarmiste. En effet, il faut convenir que les Technologies de l'Information et de la Communication permettent de tout savoir sur nos « vies numériques » et de connaître beaucoup de nos habitudes mais ils aussi pourraient servir « toute la collectivité [811]». Par exemple, l'industriel Apple intègre une application de santé qui permet une gestion de son état de santé en intégrant des fonctionnalités (payantes) qui mesurent la pression sanguine, le rythme cardiaque etc. ; de même, la société *Proteus* a investit plusieurs millions de dollars pour mettre au point un capteur ingestible qui permet de mesurer des dizaines de paramètres (acidité, douleurs, contraction) directement récupérés par un capteur sans fil, lequel transmettrait ces informations directement au médecin[812]. Néanmoins, ces nouveaux opérateurs, qui agissent à titre privé, ne doivent pas (toujours) être perçus comme une menace ; c'est, du moins, la position du vice-président du CNOM qui y voit un réel potentiel bénéfique pour la collectivité[813].

229. Une régulation institutionnelle.- Une régulation par les autorités est une solution pour que les garanties disposées par la loi, comme la « LIL » et *in fine* par le Code de la santé publique, soient effectives. C'est ce que prévoit l'article 193 de la loi de modernisation de notre système de santé du 26 janvier 2016 qui prévoit que l'Institut National des Données de Santé (INDS) soit une autorité dont la mission est de veiller à ce que les données de santé à caractère personnel soient utilisées moyennant un processus d'anonymisation fiable[814]. Cette action menée par l'INDS a aussi reçu l'appui de la CNIL qui, comme on l'a vu[815], se chargera d'assurer le processus de conformité technique et de sécurisation.

---

[810] Ibidem page 38.
[811] G. Babinet, « *Big Data*, *penser l'Homme et le monde autrement »,* 2015, éd. Le Passeur, p. 64.
[812] Voir à ce sujet, Y. Jarlaud, « *l'industrie pharmaceutique fait sa révolution… numérique »,* Collectif santé numérique, 26 janvier 2013, www.collectifsantenumerique.org.
[813] Dr J. Lucas, « *Les enjeux du Big Data dans le domaine de la santé »,* Ethique et société, Vol. 16, n°16, Mars 2016.
[814] Loi n°2016-41 du 26 janvier 2016, chapitre II, JORF n°0022.
[815] Cf. supra les exemples de procédés approuvés par la Commission.

230. L'exemple américain[816] permet d'ouvrir une réflexion sur la mise en place d'une régulation institutionnelle. Depuis 1996, les Etats-Unis (USA) ont adopté une loi qui s'applique au niveau fédéral. Cette loi dite HIPAA concerne les données de santé traitées par différents acteurs économiques dont les assurances et les entreprises permettant le traitement des données de santé via les TIC. Cette loi impose notamment au responsable du traitement d'informer et de demander le consentement du patient ou de l'utilisateur, lorsque le transfert des données est envisagé. Il impose surtout de délivrer toutes les informations à la personne concernée pour qu'elle puisse exercer pleinement ses droits[817]. Il est à noter que la revente des données de la personne concernée par le traitement ne peut être effectuée qu'après son consentement exprès et recueilli de façon distincte[818] de tout document. En outre, les USA ont mis en place un moyen de régulation grâce au régime relatif aux dispositifs médicaux, et gérés par la Food and Drug Administration (FDA), qui a une acception plus large des dispositifs médicaux. En effet, selon l'agence américaine : est un dispositif médical « tout objet ou logiciel dont l'usage prévu est soit le diagnostic d'une maladie ou d'un état de santé, soit le traitement, la guérison ou la prévention d'une maladie. [819]». Néanmoins, l'agence américaine distingue les applications de m-santé qui sont «certainement » des dispositifs médicaux de celles qui ne le sont que « peut-être ». L'objectif de la FDA est de soumettre régulièrement les applications aux critères qu'elle a définis pour retenir ultérieurement[820]la qualification de dispositif médical. La FDA a, en 2013, fait retirer du commerce le « kit génomique » mis en place par la société *23andMe* pour infraction à la législation sur les dispositifs médicaux. Or la FDA n'avait pas considéré le kit comme un dispositif médical lors de sa mise sur le marché. A l'origine, le kit génomique était présenté comme un dispositif permettant de connaître l'origine de ses ancêtres. Puis, en 2009, le kit a été présenté comme un moyen de diagnostiquer d'éventuelles prédispositions à certaines pathologies. La FDA a alors décidé de retirer le

[816] Il convient de pondérer cet exemple en indiquant que l'approche sectorielle économique des Etats-Unis permet de protéger les citoyens contre l'immixtion de l'Etat fédéral, elle permets ainsi une organisation basée sur la rédaction de chartes et de contrats organisant les relations entre les différents intervenants.

[817] US departement of health and human services National Institutes of health. HIPAA Privacy Rule and Its Impacts on Research. Disponible sur http://privacyruleandresearch.nih.gov/pr_08.asp#8a.

[818] Ibidem, voir article 7 du règlement européen du 14 avril 2016 concernant le consentement distinct de tout autre document, cf infra les nouvelles obligations du responsable du traitement

[819] Mission Economique de Chicago, « La FDA et les dispositifs médicaux », M. Alimi, S. Sutton, 29 août 2005.

[820] FDA; « Mobile Medical Applications: Guidance for Food and Drug Administration Staff », adopté le 9 février 2015.

dispositif au motif que le kit ne délivrait pas suffisamment d'informations et de conseils à l'utilisateur. La présidente de la FDA a reconnu que l'intervention de l'agence a permis de faire baisser significativement la diffusion du dispositif[821] en raison de la méfiance qu'avait suscitée la recommandation de l'agence.

En France, le Dr. J. Lucas affirme que cette régulation serait une solution car elle pourrait permettre une régulation grâce à la prescription et l'accompagnement des patients. Il s'appuie[822] sur les constatations de la CNIL[823] qui attire l'attention sur les risques de « l'hyper connexion[824] » des patients. La CNIL serait une alliée de choix de l'INDS pour réguler les nouveaux moyens de traitements de données de santé à caractère personnel en dehors du DMP. Cette régulation doit se baser[825] sur une information complète[826] des personnes car, comme le remarque R. Picard, les utilisateurs « perçoivent [827]» le fait que « rien sur le plan légal, ne peut empêcher les GAFA d'utiliser les données que les gens mettent spontanément à leur portée[828] » et d'en tirer des bénéfices économiques.

231. Une régulation citoyenne après le traitement.- S'il est capital que la gouvernance de telles données soit assurée par l'autorité publique afin d'assurer un usage éthique des données de santé à caractère personnel, de nombreux auteurs[829] indiquent que, si le bon sens impose que ces données soient naturellement couvertes par le secret, il est difficile de connaître la « priorité du citoyen éclairé dans ce domaine [830]». Sur la base des travaux de la CNIL en tant qu'autorité de contrôle, il serait également envisageable que la CNIL puisse délivrer, avec le concours de l'INDS, un label de certification et de conformité des applications. Cette certification serait d'autant plus légitime que la CNIL a

---

[821] The Guardian, « 23andMe admits FDA order 'significantly slowed up' new customers », 9 mars 2014.
[822] Dr J. Lucas, « *Les enjeux du Big Data dans le domaine de la santé »,* Ethique et société, Vol. 16, n°61, Mars 2016 ; Rapport CGEIET page 26, op. cit. loci.
[823] CNIL, délibération n°2011-035, prononçant une sanction pécuniaire à l'encontre de la société *Google inc.,* du 17 mars 2011.
[824] Dr J. Lucas, « *Les enjeux du Big Data dans le domaine de la santé »,* op. cit. loci.
[825] Nous soulignons.
[826] Appelée « literacy » outre manche, qui se décline sous forme de campagnes massives d'informations.
[827] Rapport CGEIET page 26, op. cit. loci.
[828] Dr J. Lucas, « *Les enjeux du Big Data dans le domaine de la santé »,* op. cit. loci.
[829] Ibidem notes précédentes.
[830] « 45% des consommateurs se disent préoccupés par l'utilisation abusive de leurs données lorsqu'ils se servent d'un dispositif mobile pour des activités liées à la santé. » Livre vert sur la santé mobile, 10 mars 2014.

été consultée sur les mesures techniques d'interopérabilité des systèmes lors de la mise en place du DMP[831]. C'est le concept qui a été développé par l'Association des Hôpitaux de New York qui a mis en place une plateforme nommée « HAPPTIQUE » qui applique quatre critères déterminants relatifs à la fiabilité des applications : « des normes d'opérabilité, des normes de protection de données personnelles, des normes de sécurité et des normes relatives aux contenus.[832] »

En l'espèce, il serait envisageable, compte tenu des prérogatives de la Commission, que cette dernière applique les normes prévues en matière d'interopérabilité[833] afin que l'utilisateur puisse souscrire à des logiciels autorisant, si nécessaire, un accompagnement de l'utilisateur dans la gestion de ses données de santé à caractère personnel. En effet, la mission générale de la CNIL est un devoir d'information à l'égard du public concerné par le traitement des informations à caractère personnel. Les dispositions de la Loi du 6 janvier 1978 indiquent que la CNIL remplit une mission de contrôle, d'élaboration et de mise en œuvre de traitement des informations *a priori* mais également *a postériori* comme en dispose l'article 11 de le loi n°78.17 du 6 janvier 1978 qui donne à la Commission le pouvoir de veiller « à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi. ». Les traitements automatisés portant sur les données sensibles sont soumis à une autorisation préalable de la Commission, mais, également, lorsque l'objet du traitement doit permettre « l'interconnexion de fichiers »[834]. De même, on a vu que la CNIL a un pouvoir de contrôle concernant les méthodes de sécurisation des données[835].

Conclusion.- Quoi qu'il en soit, l'usage de ces technologies hors du cadre d'une prise en charge classique, nécessitera une information claire, loyale et détaillée sur leurs fonctionnalités et conditions d'utilisation qui font l'objet d'un encadrement de droit *commun* par la loi «Informatique et Libertés» visé à l'article 32. Cet encadrement et l'ajout

[831] CNIL, avis 2016-147 portant avis sur un projet de décret pris en Conseil d'Etat relatif au Dossier Médical Partagé, du 12 mai 2016.
[832] CNIL, Cahiers IP2, « *Le corps, nouvel objet connecté du quantified self à la m-santé : les nouveaux territoires de la mise en données du monde* », 2014, page 48.
[833] La CNIL devra se prononcer notamment sur le déploiement des Référentiels Généraux de Sécurité (RGS) et des Référentiels Généraux d'Interopérabilité (RGI) comme en dispose l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
[834] Article 25 de le loi 78.17 du 6 janvier 1978.
[835] Cf supra l'anonymisation à bref délai.

d'un contrôle spécifique[836] de la part des autorités permettraient la mise sur le marché d'outils de m-sante comportant des garanties pour leurs utilisateurs, notamment le droit de s'opposer, après la mise en œuvre du traitement, permettant ainsi de mettre fin à un traitement que l'utilisateur jugerait inapproprié[837]. Il serait regrettable de ne pas exploiter le potentiel que représente, en termes de santé publique, l'utilisation de nouvelles technologies telles que la santé mobile.

Par ailleurs, le Conseil des ministres des télécoms de l'UE a affirmé en 2008 la nécessité de reconnaître un « droit au silence des puces ». On parle aujourd'hui plutôt d'un « droit au contrôle » des puces. Ce droit, au-delà de la problématique générale des objets connectés, pourrait très utilement s'appliquer aux appareils de *quantified self* et garantir à leurs usagers la maîtrise de la diffusion des données personnelles produites par ces outils. Cette maîtrise des données se manifeste également par un nouveau concept développé récemment par la jurisprudence européenne dans l'arrêt dit « *Google Spain »* qui consacre un « droit à l'oubli numérique ». Ce concept sert de fondement pour le développement du nouveau projet de « république numérique » visant à mettre en place les garanties juridiques et techniques donnant naissance à une sorte de *citoyen numérique.*

Chapitre 2 : L'évolution des droits permettant la maîtrise des données à caractère personnel

A l'origine, la loi «Informatique et Libertés» du 6 janvier 1978 ne faisait pas référence à la notion de consentement, excepté en matière de données sensibles. C'est la directive européenne du 24 octobre 1995 qui est venue définir le consentement à l'article 2. Cependant, on assiste à un regain d'intérêt de la part des législateurs français et européen, qui souhaitent donner une place centrale au consentement en ce qui concerne le traitement des données de santé à caractère personnel. La notion de consentement est centrale en matière de données de santé car il permet, au patient comme à l'utilisateur, de maîtriser les informations qu'ils souhaitent communiquer ou non. L'expression du consentement permet l'exercice de prérogatives telles que le droit d'accès dont le champ d'application est très

[836] Contrôle effectué par la CNIL et la COFRAC permettant une certification cf supra « la procédure d'agrément ».

large et qui est le pendant, selon la CNIL[838], du droit à l'oubli (Section 1). L'évolution des garanties juridiques, permettant l'effectivité du droit des personnes semble dessiner les contours d'un « Habeas Corpus » numérique, tant en droit français qu'en droit européen (section 2).

Section 1 : La consécration de nouveaux moyens de maîtrise des données

Comme visé à l'article 1er de la « LIL » l'informatique doit être au service de l'homme et non l'inverse. Néanmoins, nos *traces* référencées sur internet peuvent être préjudiciable pour la personne concernée. C'est sur le fondement de ce postulat que la CJUE a dégagée un droit *à l'oubli* (a). Ce droit a été intégré lors de la rédaction du nouveau Règlement européen du 27 avril 2016, mais ne doit pas être confondu avec le droit d'opposition (b).

a) Du droit à l'oubli

Afin d'illustrer l'enjeu d'un tel droit, on peut citer la formule du président de l'INA, qui, en 2001, constate déjà que nous sommes face à une « hypermnésie » d'internet. Il ajoute, dans son ouvrage[839], que le droit à l'oubli est le « seul socle sur lequel une nouvelle démocratie peut être fondée ». Il considère que la société numérique est en crise et qu'il est capital de « civiliser cette nouvelle mémoire [840]» collective. Comme la CNIL[841], l'auteur affirme que le « droit des réseaux » doit concourir à un effacement périodique et « définitif » des données collectées. La Commission considère que le droit à l'oubli doit se comprendre comme étant le *Droit* « de changer, d'évoluer » et de « se contredire [842]».

Au-delà de ces considérations philosophiques il convient, au travers de l'évolution de la notion du droit à l'oubli, d'étudier les sources, le contenu et les prérogatives attachées au droit à l'oubli.

232. Les sources du droit à l'oubli.- La CNIL a souvent évoqué cette notion et considère qu'elle est le fruit de la construction juridique relative aux droits de la personnalité, et, plus précisément, du droit au respect de la vie privée. L'atteinte au droit à

[838] CNIL, 35ème Rapport annuel d'activité 2014, disponible sur www.cnil.fr.
[839] E. Hoog, « Mémoire année zéro », édition seuil, coll. Essais, 2009.
[840] A. Koukoutsaki-Monnier, « Emmanuel HOOG, *Mémoire Année Zéro* », *Questions de communication* [En ligne],17 | 2010, mis en ligne le 23 janvier 2012, consulté le 27 juillet 2016. URL : https://questionsdecommunication-revues-org.biblio-dist.ut-capitole.fr/239.
[841] CNIL, 35ème rapport d'activité op. cit . loci.
[842] CNIL, guide « informatique et libertés » pour l'enseignement du second degré, 2010.

la vie privée se manifeste, le plus souvent, lorsque des éléments de la vie privée de la personne sont à nouveau publiés alors que les faits avaient été révélés quelques années auparavant. Ce nouveau cas de révélation intervient, notamment, dans la presse, lorsqu'il est effectué un parallèle avec des éléments d'actualité. En matière de presse, cette nouvelle publication se justifie par l'existence d'une nécessité d'information et sous réserve de ne pas porter atteinte à la dignité humaine[843]. Dans ces circonstances, la qualification d'atteinte à la vie privée ne peut pas être retenue.

Cependant, lorsque ces éléments sont publiés ou utilisés sans le but d'illustrer un événement devenu historique, leur publication sans autorisation peut constituer une atteinte à la vie privée. Or, il apparaît légitime que la personne concernée par la publication de faits intervenus dans le passé veuille « se faire oublier » [844] ou ne veuille pas subir « le rappel intempestif d'un passé douloureux[845] ». Le droit à l'oubli est donc le prolongement de l'article 9 du Code civil qui protège le droit de tout un chacun de décider de ce qui relève de sa vie privée.

233. Le droit à l'oubli appliqué aux données à caractère personnel.- Selon la CNIL, l'existence du droit à l'oubli ne fait aucun doute, en ce sens où elle l'énonce clairement ce droit dans une délibération en affirmant que « face à la mémoire de l'informatique, seul le principe du droit à l'oubli, consacré par l'article 6, 5°) de la loi du 6 janvier 1978, peut garantir que les données collectées sur les individus ne soient pas conservées [846]». C'est sur le fondement du droit à l'oubli que la Commission considère qu'une entreprise ne peut conserver de manière « manifestement excessive » les données qui concernent ses clients[847]. Si l'on se réfère au fondement invoqué par la Commission qui est que le droit à l'oubli est fondé sur la nécessité de déterminer la finalité du

---

[843] Cass. Civ. 1ère, n°99-15970, 20 février 2001, bull. 2001 I n°43 ; D. 2001 JSP 1199 note J-P Gridel p. 1990, note A. Lepage ; Cass. Civ. juillet 2001, D.2002 jur 1380 note C. Bigot, p. 22298 observation L. Marino ; Cass. Civ. n°00-19403, 13 novembre 2003, bull. 2003 I n°231 p. 183, « *Les Droits de la personnalité à l'épreuve des grandes affaires criminelles »,* A. Lepage, D. 2004, p. 1634. ; Article 35 de la loi du 29 juillet 1881 sur la liberté de la presse qui incrimine la diffusion de la reproduction des circonstances d'un crime ou d'un délit, lorsque cette reproduction porte gravement atteinte à la dignité humaine d'une victime et qu'elle est réalisée sans l'accord de l'intéressé.

[844] B. Beigner, « *Le droit de la personnalité* », Coll. *Que sais-je*. n°2703, éd. Puf , novembre 1992.

[845] C. Caron, « *A propos du conflit entre les œuvres de fiction et la vie privée »*, D. 2003, jur, P. 1715.

[846] CNIL, délibération n°2005-213 portant adoption d'une recommandation concernant les modalités d'archivage électronique dans le secteur privé de données à caractère personnel, du 11 octobre 2005.

[847] *Ibidem*.

traitement[848], la CNIL considère que le droit à l'oubli doit être mentionné (à la personne concernée) lors de l'accomplissement de l'obligation d'information par le responsable du traitement[849]. Il s'agit de comprendre que cette position est fondée sur le fait qu'une fois la finalité du traitement atteinte, un nouveau traitement de ces dernières ne peut être admis. C'est-à-dire que la conservation des données ne doit pas pouvoir permettre l'identification des personnes concernées par le traitement au-delà de la durée nécessaire aux finalités pour lesquelles les données sont collectées et traitées[850]. Comme on l'a vu, si un nouveau traitement doit être effectué, la personne concernée devra en être informée. C'est le raisonnement sur lequel la CNIL s'est appuyée pour fonder sa délibération concernant l'anonymisation des décisions de justice publiées sur internet[851]. C'est également sur la combinaison des articles 6, 5°) et 24 de la « LIL » de 1978 que la Commission fixe la durée de conservation des données lors de l'adoption des normes simplifiées. La Commission fonde ses décisions, non pas sur le respect du droit à la vie privée, mais, sur le principe d'une durée de conservation proportionnée à la finalité poursuivie[852].
Si la CNIL et la doctrine[853] ne contestent pas l'existence du droit à l'oubli, la nature de ce droit n'a pas toujours le même fondement.

234. Le droit à l'oubli corollaire du droit de suppression.- En 2009, le droit à l'oubli a été envisagé lors d'une proposition de loi. En effet, le rapport[854] « Detraigne Escoffier » voit dans la consécration d'un droit à l'oubli numérique une garantie supplémentaire de mieux « protéger le droit à la vie privée à l'heure du numérique ». Les rapporteurs insistent sur la nécessité de la mise en place de logiciels faisant l'objet d'une labellisation. Ils insistent également sur la nécessité de promouvoir des systèmes permettant aux utilisateurs de « supprimer » leurs données, sans subordonner cette prérogative à l'exigence d'un motif légitime. Les conclusions du rapport indiquent que l'exercice de ce droit doit pouvoir se faire par voie électronique, par opposition à

[848] Article 6, 5°) de la « LIL » de 1978 op. cit. loci.
[849] CNIL, délibération n°2005-213 du 11 octobre 2005, op. cit. loci.
[850] Cf supra, La finalité du traitement.
[851] CNIL, délibération n°01-057 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence, du 29 novembre 2001.
[852] Article 30, 5°) de la « LIL » modifiée, op. cit. loci. ; Délibération n°2005-213 op. cit. loci.
[853] F. Meuris-Guerrero, « *Une clarification du droit au déréférencement »,* Comm. Com. Electr. N°12, Décembre 2015 ; M. Vivant, « *Un droit à l'oubli »,* Le Lamy droit du numérique, n°598, 2016.
[854]« *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information* », Rapport d'information de Y. Détraigne et A-M. Escoffier, fait au nom de la commission des lois, n° 441 (2008-2009), 27 mai 2009.

l'exigence de certains responsables du traitement qui exigeaient que cette demande soit effectuée par courrier postal, ce qui « peut décourager » la personne concernée par le traitement d'user de son droit à ce que ses données soient supprimées. Enfin, les rapporteurs ajoutent que ce droit devrait se distinguer du droit d'opposition commerciale qui permet, notamment, de s'opposer à ce que les données soient transférées à d'autres entreprises[855].

235. Les recommandations du G29.- Selon le groupe de travail[856], les données personnelles déposées par l'utilisateur, sur un service en réseau, devraient être supprimées dès que le responsable du traitement décide de supprimer le compte. De même, le G29 insiste sur le fait que, si l'utilisateur est à l'origine de cette suppression, les données ne devraient être conservées que pour des raisons de sécurité ou d'obligation légale et pour une durée déterminée. En effet, « il pourrait être justifié de conserver pour une durée déterminée des données qui ont été mises à jour ou effacées et des comptes afin d'empêcher les opérations malveillantes résultant de l'usurpation d'identité et d'autres délits [857]». Lorsque le titulaire effectue une simple mise à jour de son compte, les données antérieures à cette opération doivent être supprimées ou du moins devenir inaccessibles aux autres utilisateurs[858].

236. La Charte du droit à l'oubli.- Le 13 octobre 2010, la secrétaire d'Etat chargée de la Prospective et du Développement de l'Economie Numérique prévoyait que les moyens donnés aux utilisateurs devaient permettre, dès la collecte des données, une information « claire, transparente, complète et facile à retrouver sur le site, sur la durée de conservation des données à caractère personnel [859]». La charte du droit à l'oubli a pour fondements les articles 6, 4°) 5°), 36 alinéa 1er et 40 alinéa 1er de la loi «Informatique et Libertés» modifiée. L'objectif de cette charte est de « matérialiser les principes [860]» de finalité du traitement et de permettre la manifestation concrète du consentement, du droit à l'information, du droit d'accès, de rectification et d'opposition, prévus par la « LIL ». Cette

[855] Rapport, n° 441 (2008-2009), 27 mai 2009, op. cit . loci.
[856] G29, Avis 5/2009 « sur les réseaux sociaux en ligne », adopté le 12 juin 2009, WP 163.
[857] M. Vivant, « *Un droit à l'oubli »,* Op. cit. loci.
[858] G29, Avis 5/2009 op. cit. loci. Voir, N. Mallet-Pujol, « *Droit à l'oubli numérique et désindexation : la solution en trompe l'œil de CJUE »*, Chroniques et opinions, Droit de la personnalité, Légipresse, 2014, n°319.
[859] Article 1.3 de la Charte Du Droit A L'oubli dans les sites collaboratifs et les moteurs de recherche, 13 octobre 2010.
[860] Préambule de la Charte op. cit. loci.

charte avait pour objectif de réunir le plus grand nombre d' « acteurs imposants » sur internet. Cependant, les entreprises les plus influentes d'internet, c'est-à-dire *Facebook* et *Google,* n'ont pas signé cette charte.

Enfin, reste la question des données anonymes qui échappent à la qualification de données à caractère personnel. La charte du droit à l'oubli propose de limiter la conservation et l'exploitation des *cookies* à une durée de 60 jours par défaut. L'innovation remarquable est la création d'un bureau unique de réclamation qui permettrait une harmonisation des moyens de contrôle des données en les centralisant.
Ce qui prive la charte, initiée par Mme N. Kosciusko-Morizet, de valeur contraignante[861] est le fait que les deux géants d'internet n'ont pas adhéré à la mise en place de ces recommandations ; cependant, l'entreprise *Google* a été contrainte, en 2014, de reconnaître le droit à l'oubli, grâce à l'interprétation de la CJUE[862] des articles 12 et 14 de la directive 95/46/CE du 20 octobre 1995[863].

237. L'apport de la CJUE.- Afin de saisir l'étendue de la problématique, il convient de rappeler les faits qui ont permis à la Cour de Justice Européenne de fonder en droit sa décision. En 1998, M. Costeja Gonzalez a fait l'objet d'une saisie immobilière et un journal avait publié une annonce relative à cette adjudication comportant son nom. En 2009, alors que la procédure était close depuis de nombreuses années, le plaignant était toujours indexé dans les résultats du moteur de recherche de *Google* qui renvoyaient aux pages du journal des adjudications judiciaires. L'AEPD[864] rejeta le recours contre le journal mais a demandé que soit retirées les informations litigieuses. En 2013, l'avocat général de la CJUE a fait droit à la demande de l'entreprise américaine, sur le fondement de la liberté d'expression en indiquant que faire supprimer des informations qui sont, de manière légitime, « *entrées dans la sphère publique serait constitutif d'une ingérence dans la liberté d'expression de l'éditeur de la page Web*[865] *»*.

---

[861] D. Seddiki, « *Premiers enseignements du droit à l'oubli », Droit de l'Homme et Libertés fondamentales,* village-justice.com, 1 octobre 2014 ; Thiérache C., « *Le droit à l'oubli numérique : un essai qui reste à transformer* », RLDI 2011/67, n° 2188.
[862] CJUE, affaire C-131/12, Google spain SL et Google Inc. contre Agencia Española de Protection de datos (AEPD) et Mario Costeja Gonzàlez, 13 mai 2014.
[863] Respectivement ces articles visent le droit d'accès et le droit d'opposition de la personne.
[864] Agencia Española de Protección de Datos.
[865] Conclusions de l'avocat Général M. Niilo Jääskinen présentées le 25 juin 2013, Google Spain SL Google Inc. Contre Agencia Española de Protección de Datos (AEPD) Mario Costeja González.

La grande chambre de la CJUE indique que le droit à l'oubli ne peut s'analyser comme un pouvoir « discrétionnaire [866]» de la personne concernée, c'est-à-dire qu'elle ne peut exiger que soient supprimées les données accessibles au public. En effet, le juge subordonne la suppression des données à la démonstration, de la part de l'utilisateur, que les données litigieuses sont « inadéquates », « pas pertinentes » ou excessives « au regard de leur finalité initiale[867] ».

Néanmoins, il ressort de l'arrêt qu'il appartiendra à l'autorité administrative et au juge national de déterminer, en cas de contentieux, si la personne est une personne publique ou non et d'apprécier si les informations en cause présentent une valeur en tant qu'*Informations* vis-à-vis du public. La CJUE semble appréhender ce droit dans un but de régulation de la liberté d'expression et non dans le but de protéger le droit à la vie privée. Cet arrêt semble poser les bases d'un nouveau droit mais nécessite une clarification[868].

238. La nature du droit à l'oubli.- Dans son 35ème rapport d'activité, la CNIL indique que le droit à l'oubli est en réalité un droit au déréférencement et serait en réalité une déclinaison du droit d'accès consacré par la « LIL » de 1978. La Commission affirme, dans son rapport, que l'activité des moteurs de recherche est un traitement de données à caractère personnel au sens de l'article 2, b) de la directive 95/46/CE. La Commission exclut ainsi l'argument qui tend à ne pas qualifier les moteurs de recherche de responsables du traitement, au motif qu'ils ne sont pas à l'origine de la création des données collectées[869]. Toujours selon la CNIL, sur le fondement des articles 12 et 14 de la directive 95/46/CE de 1995, lorsque les données ont été rendues publiques, la personne concernée doit avoir le droit d'obtenir le déréférencement, sans avoir à invoquer préalablement le droit à l'effacement. En d'autres termes, ce droit doit pouvoir s'exercer sans exiger un motif légitime invoqué par la personne concernée, contrairement au droit de suppression ou de rectification[870]. Ainsi, la CNIL affirme que le droit au déréférencement est un droit qui s'exerce de façon autonome mais qui n'entraîne pas la suppression automatique des données. Il doit faire l'objet d'une analyse au cas par cas, en fonction de la qualité et de la

[866]Affaire C-131/12, *Google Spain* op. cit. loci.
[867] Ibidem.
[868] N. Mallet-Pujol, « *Droit à l'oubli numérique et désindexation : la solution en trompe l'œil de CJUE »*, Chroniques et opinions, Droit de la personnalité, Légipresse, 2014, n°319.
[869] 35ième rapport CNIL op. cit. loci. ; M. Vivant, « Qu'est-ce qu'être « responsable de traitement ? », Guide pratique Lamy Droit du numérique 2016, Le Lamy droit des médias et de la communication n°4255 ; F. Meuris-Guerrero, « *Une clarification du droit au déréférencement et la naissance d'un droit des drones* », Comm. Com. Electr. n°12, décembre 2015.
[870] Article 38 de la « LIL » modifiée.

fonction de la personne concernée par la publication d'informations. La CNIL reprend les critères retenus par le G29. En effet, le Groupe de travail[871] indique que lorsque le droit au déréférencement est invoqué, il s'agit de déterminer si :

« - Les résultats de recherche sont-ils relatifs à une personne physique ?
- Le résultat apparaît-il à la suite d'une recherche effectuée à partir du nom de la personne concernée ?
- S'agit-il d'une personne publique ? Le plaignant joue-t-il un rôle dans la vie publique ?
- Le plaignant est-il mineur ? Les données sont-elles exactes ?
- Les données sont-elles pertinentes et/ou excessives ?
- L'information est-elle sensible au sens de l'article 8 de la directive 95/46/CE ?
- L'information est-elle à jour ? L'information a-t-elle été rendue disponible plus longtemps que nécessaire pour le traitement ?
- Le traitement de l'information cause-t-il un préjudice au plaignant ? Les données ont-elles un impact négatif disproportionné sur la vie privée du plaignant ?
- Les informations issues du moteur de recherche créent-elles un risque pour le plaignant?
- Dans quel contexte l'information a-t-elle été publiée ?
- Le contenu a-t-il été rendu public à des fins journalistiques ?
- La publication de l'information répond-elle à une obligation légale ? L'auteur de la publication avait-il l'obligation de rendre cette donnée personnelle publique ?
- L'information est-elle relative à une infraction pénale ? [872]»

Il convient de noter que, même si un préjudice n'est pas la condition *sine qua non* à l'exercice de ce droit, l'existence d'un préjudice « oriente » vers un déréférencement de l'information[873]. Compte tenu de l'apparition récente de la notion, il convient d'étudier le droit au déréférencement dans le nouveau Règlement Européen qui a pour objet un renforcement des droits existants et qui contient de nouvelles prérogatives notamment concernant le droit à l'oubli.

b) L'apport du nouveau Règlement européen

[871] G29, Working Document 228, « *On surveillance of electronic communications for intelligence and national security purposes*. », adopté le 5 décembre 2014.
[872] CNIL, rapport sur le droit au déréférencement, « Les critères communs utilisés pour l'examen desplaintes »,2014,https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf.
[873] F.Meuris-Guirrero, « Une clarification du droit au déréférencement », op.cit.loci.

239. Du droit à l'oubli au droit à l'effacement.- Il semble que la terminologie ait nécessité une clarification. En effet, en 2013, la Commission LIBE a renommé le droit à *l'oubli* en droit à *l'effacement* en invoquant comme argument que, si une personne demande à un responsable du traitement (par exemple, une entreprise d'Internet) d'effacer ses informations personnelles, l'entreprise devra également envoyer la demande aux parties qui dupliquent les données[874]. Ainsi, ce « droit à l'effacement couvrirait le droit à l'oubli proposé par la Commission européenne [875]».

240. Le droit à l'effacement dans le Règlement européen 2016/679.- Le droit à l'effacement est visé à l'article 17 du Règlement européen adopté 27 avril 2016[876] et dispose que « la personne concernée [par le traitement] a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais ».

241. Les conditions d'exercice du droit à l'effacement.- L'article 17 §1 du Règlement prévoit six cas dans lesquels la personne peut exercer le droit à l'effacement. Ainsi, ce droit peut s'exercer lorsque « les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière[877] », « la personne concernée retire le consentement sur lequel est fondé le traitement [878]», « la personne concernée s'oppose au traitement en vertu du droit d'opposition[879] », de même s'« il n'existe pas de motif légitime impérieux pour le traitement [880]», « les données à caractère personnel ont fait l'objet d'un traitement illicite [881]», « les données à caractère personnel doivent être effacées pour respecter une

---

[874] Considérant n°66 du Règlement du Parlement européen et du Conseil, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, du 27 avril 2016, n°2016-679, JOCE 119/1.
[875] Communiqué de presse de la Commission LIBE, 22 octobre 2013.
[876] Règlement du Parlement européen et du Conseil, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, du 27 avril 2016, n°2016-679, JOCE 119/1.
[877] Article 17 §1, a) du Règlement op. cit. loci
[878] Article 17 §1, b) du Règlement op. cit. loci
[879] Article 21 §1 du Règlement op. cit. loci.
[880] Article 17 §1, c) du Règlement op. cit. loci.
[881] Article 17 §1, d) du Règlement op. cit. loci.

obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis[882] » et enfin lorsque « les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information [883]» nécessitant la collecte d'informations d'un mineur. Le législateur européen fait ici un véritable apport en ce qui concerne les informations collectées lorsque la personne concernée était mineure. Elle permet la possibilité à la personne concernée de demander l'effacement des données rendues disponibles « lorsqu'elle était enfant ». L'article 8 §1 précise que le traitement des données est licite lorsque la personne mineure est âgée d'au moins 16 ans. Cependant, le règlement laisse la possibilité aux Etats membres de prévoir une limite inférieure qui ne peut aller en deçà de 13 ans[884].

Le Règlement européen ne subordonne pas l'exercice de ce droit à la justification d'un motif légitime, ce qui aurait pour effet de « vider de son sens » cette prérogative. En effet, « s'il est possible de comprendre le refus de tout droit à l'oubli lorsque ce dernier entre en conflit avec un intérêt concurrent tel que la recherche historique, ce refus est difficilement justifiable lorsqu'il n'y en a pas. Sans un intérêt concurrent légitime, il est difficile, en effet d'expliquer cette volonté de conserver des informations contre la volonté de la personne concernée[885] ».

242. La portée du droit à l'effacement (*droit à l'oubli*).- L'application du droit à l'effacement n'entraîne pas une suppression automatique des données litigieuses. En effet, ce droit entraîne la cessation de la diffusion des données, c'est-à-dire la suppression des liens permettant d'accéder aux informations. Cette cessation de la diffusion est visée à l'article 18 §1 du Règlement. Cette disposition s'apparente à un « gel » de la diffusion des données durant lequel le responsable du traitement peut vérifier l'exactitude des données contestées. L'exercice de ce droit permet de rendre indisponible les données qui ne peuvent faire l'objet d'un traitement[886]. Cependant, lorsque le responsable du traitement estime que l'information peut faire à nouveau l'objet d'un traitement, il doit avertir la personne concernée et obtenir son consentement. Le droit à l'effacement consacré par le règlement

[882] Article 17 §1, e) du Règlement op. cit. loci.
[883] Article 17 §1, f) du Règlement op. cit. loci.
[884] Notons ici que l'âge minimum retenu dans le règlement est le même qui est exigé pour l'inscription sur le site *Facebook.*
[885] Vers la mise en place d'un droit à l'oubli numérique, le Lamy droit des medias et de la communication, n°477-50 ; Berguig M., Thiérache C., L'oubli numérique est-il de droit face à une mémoire numérique illimitée ?, RLDI 2010/62, no 2039 ; Bensoussan A., Le droit à l'oubli sur Internet, Gaz. Pal., 6 févr. 2010, no 37, p. 3.
[886] Article 18 §2 du Règlement op. cit. loci.

fait donc peser une nouvelle obligation sur le responsable du traitement. En effet, l'exercice de ce droit apparaît comme une prérogative *alternative* au droit d'opposition, permettant de rendre temporairement inaccessibles les informations. Cet effacement *temporaire* oblige le responsable du traitement à vérifier l'exactitude des données, mais aussi, à apporter (de nouveau) la preuve de la licéité du traitement. Ainsi, le responsable pourra invoquer les exceptions prévues par l'article 17 §3 du règlement qui prévoit 6 exceptions permettant d'écarter le droit à l'effacement. Ainsi, ce droit n'a pas vocation à s'appliquer dans la mesure où le traitement est nécessaire « à l'exercice du droit à la liberté d'expression et d'information[887] », à l'exercice d'une obligation légale qui requiert le traitement « prévu par le droit de l'Union » ou par le droit d'un Etat membre[888], pour une mission d'intérêt public, pour une mission de santé publique, aux fins « archivistiques », de recherche scientifique, historique[889] et enfin si le traitement est nécessaire à la constatation et l'exercice de droits en justice[890].

243. Véritable apport ou redondance ?- Il s'agit de distinguer le droit au déréférencement (droit à l'oubli) du droit d'opposition et de suppression. Dans le cas du droit de suppression, la suppression est de plein droit, alors que le droit d'opposition doit être fondé sur un motif légitime. Certains auteurs[891] estiment que le droit à l'oubli n'est pas nécessaire compte tenu de l'existence légale d'une limite dans la conservation des données et du principe de finalité du traitement. En outre, le droit à l'oubli, tel qu'envisagé par le règlement, peut également se rapporter à la nature illicite du traitement, visé par les articles 6 et 7 de la « LIL » de 1978, lorsque celui-ci porte atteinte aux droits et aux libertés des personnes, entraînant, de fait, que le responsable ne puisse plus se prévaloir de son l'intérêt légitime à effectuer le traitement.

Il n'en demeure pas moins que le droit à l'effacement, prévu par l'article 17 du Règlement, permet à la personne concernée par le traitement de faire cesser, au moins temporairement, le trouble que la publication provoque. Cette prérogative de la personne concernée permet une maîtrise directe de la personne sur ses données. Cette maitrise se justifie d'autant plus

[887] Article 17 §3, a) du Règlement op. cit. loci.
[888] Article 17 §3, b) du Règlement op. cit. loci.
[889] Article 17 §3, c) du Règlement op. cit. loci.
[890] Article 17 §3, d) du Règlement op. cit. loci.
[891] Vers la mise en place d'un droit à l'oubli numérique, le Lamy Droit des Medias et de la Communication, n°477-50 ; Berguig M., Thiérache C., L'oubli numérique est-il de droit face à une mémoire numérique illimitée ?, RLDI 2010/62, no 2039 ; Bensoussan A., Le droit à l'oubli sur Internet, Gaz. Pal., 6 févr. 2010, no 37, p. 3. ; N. Metallinos, « Réforme du cadre européen de la protection des données à caractère personnel : où en est-on ? » RLDI 2013, n°99, décembre 2013.

par « l'expansion des données qui comportent » des empreintes numériques[892]. Il conviendra de s'en remettre au principe dégagé par l'arrêt *Google Spain* qui permet de garantir l'équilibre entre les droits fondamentaux de la personne et la liberté d'expression[893].

Section 2 : La création d'un Habeas Corpus numérique

Le projet de loi permettant de fonder une *République Numérique,* qui a été présenté par le gouvernement et la secrétaire d'Etat chargée du numérique A. Lemaire le 15 décembre 2015[894], a pour ambition de renforcer, du moins sur les principes, les droits attachés à la personne. En effet, lors de sa présentation, il a été rappelé que ce projet a été élaboré grâce à un processus « de co-construction » au travers d'une « grande concertation nationale » et initié par le premier Ministre. En effet, lors de l'exposé des motifs, le Gouvernement a indiqué qu'il souhaitait « proposer un cadre nouveau, qui combine soutien à l'innovation et aux nouveaux modèles économiques, ouverture élargie des données, protection renforcée des personnes, renforcement de la loyauté des plateformes et déploiement de l'accès au numérique. [895]». En outre, l'ambition de ce projet est de permettre « l'égalité » d'accès aux technologies de l'information et de défendre un droit « à l'accès à internet » pour tous les citoyens. Le projet proposait de renforcer les droits des utilisateurs, notamment en développant un cadre juridique qui garantisse la loyauté et la régulation des plateformes (a). C'est avec l'appui du Conseil National du Numérique (CNNum) que la secrétaire d'Etat et le gouvernement ont proposé un renforcement de l'exercice des droits attachés à la personne « en ligne », notamment avec l'introduction de la notion de « portabilité des droits » permettant à l'utilisateur de disposer librement de ses données, non seulement dans le but de protéger son droit à la vie privée, mais, surtout, dans un but de régulation économique (b).

---

[892] P. Tucker, « *Has Big Data made anonymity impossible* ? », MIT technology review, 7 mai 2013.
[893] Arret *Google Spain,* affaire C-131/12, du 13 mai 2014 ; Rapport du Conseil d'Etat, « *Le Numérique et les Droits Fondamentaux »*, La Doc. Fr. Coll. Rapports du Conseil d'Etat, 2014, page 277.
[894] Projet de loi n°3318, *Pour une République Numérique*, présenté au nom du premier Ministre par le Ministre de l'économie, de l'industrie et du numérique et la secrétaire d'État chargée du numérique, le 9 décembre 2015.
[895] *Ibidem note préc;* voir aussi les contributions sur www.république-numérique.fr.

a) La régulation et la loyauté des plateformes

244. L'article 23 du projet de « Loi de République Numérique » (LRN) vise à inciter les plateformes dont l'audience est importante à définir la mise en place de leurs « bonnes pratiques » et à les rendre publiques. Le dispositif mis en place par le projet LRN prévoit que les plateformes doivent recourir à une auto-régulation, notamment avec la publication d'indicateurs de référence. Ces indicateurs de références seraient la possibilité pour l'utilisateur de connaître l'audience de la plateforme, mais, aussi, d'avoir connaissance des bonnes pratiques mises en place par elles. Afin de garantir l'efficacité du dispositif, l'article 23 de la LRN prévoit que le Gouvernement pourra publier une liste des plateformes dont il estime les pratiques déloyales.

245. Le dispositif.- Pour cela, le projet LRN propose la modification du Code de la consommation en insérant, à l'alinéa 1er de l'article L.111-5-1 la définition des plateformes : « est qualifiée d'opérateur de plateforme en ligne, toute personne exerçant à titre professionnel des activités consistant à classer ou référencer des contenus, biens ou services proposés ou mis en ligne par des tiers, ou à mettre en relation, par voie électronique, plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service, y compris à titre non rémunéré, ou de l'échange ou du partage d'un bien ou d'un service[896] ». Le projet fonde son dispositif sur l'article 19 de la LCEN n°2004-575 du 21 juin 2004, en ajoutant que la plateforme doit délivrer une « information loyale, claire et transparente sur les conditions générales d'utilisation ». Il semble anticiper l'application du Règlement européen en ajoutant que la plateforme doit proposer et renseigner l'utilisateur sur les « modalités de référencement, de classement et de déréférencement des contenus[897] ».

Le projet ajoute une modification du Code de la consommation en ce qui concerne les seuils de nombre de connexion. En effet, il précise que les seuils de connexion devront être établis par décret[898]. Dans le cas où une plateforme atteindrait les seuils d'audience définis par décret, elle devrait fournir à l'autorité administrative compétente la preuve qu'elle élabore et diffuse auprès des utilisateurs (consommateurs) les bonnes pratiques visant à renforcer leurs obligations de clarté, de transparence et de loyauté. Le responsable du traitement devra également démontrer que sont définis des indicateurs permettant

[896] Article 22 de projet LRN n°3318 op. cit. loci.
[897] Idem.
[898] Article 23 du projet LRN n°3318 op. cit. loci.

d'apprécier le respect de leurs obligations de clarté, de transparence et de loyauté, et, enfin, il devra rendre périodiquement publics les résultats de l'évaluation des indicateurs[899].

Le projet de loi affirme que les plateformes ont une obligation renforcée d'information à l'égard de l'utilisateur. Cette obligation est prévue par l'article 19 de la LRN qui consacre notamment le principe de « neutralité » d'internet. Selon le projet de loi, la neutralité des réseaux et d'internet « consiste à garantir l'accès à l'internet ouvert régi par le règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union. »

Le projet de LRN fait explicitement référence au nouveau Règlement européen relatif à la protection et à la circulation des données à caractère personnel au sein de l'Union Européenne.

Le dispositif développé par le projet de LRN est, en réalité, une application de l'étude réalisée par le Conseil d'Etat sur « *les droits fondamentaux et le numérique*[900] » en 2014 qui constate que l'organisation en plateformes des réseaux, dont la « logique économique » pousse à la constitution d'ensembles « toujours plus importants », nécessite le développement ou le renforcement d'outils juridiques, notamment concernant la nécessité d'informer les utilisateurs[901].

246. La loyauté garantie par la CNIL.- Sans revenir sur les pouvoirs de contrôle de la Commission exposés précédemment, le projet de LRN prévoit, à l'article 29, la modification de la « LIL » n°78-17 du 6 janvier 1978. En effet, l'article 11 de la « LIL » serait ainsi modifié en donnant le pouvoir à l'AAI d'être automatiquement saisie lorsqu'un projet de loi concernerait la protection des données à caractère personnel. Cependant, le projet de LRN apporte une mission supplémentaire à la CNIL en matière de chiffrement des données. En effet, le projet de loi LRN renforce les missions de la Commission à l'article 37 de « LIL » de 1978 modifiée, qui prévoit qu'elle est habilitée à « certifier » les

[899] Article 23 du projet LRN n°3318 op. cit. loci. Modifiant l'article L. 111-5-2 §I du Code de la consommation (Abrogé par l'ordonnance n°2016-301 du 14 mars 2016).
[900] Etude annuelle 2014 du Conseil d'État, La Doc. Fr. Coll. Rapports publics page 156.
[901] « Si toutes ces informations restaient disséminées auprès des personnes qui les ont recueillies, les risques pour la vie privée seraient sans doute limités. La dynamique de l'économie numérique pousse cependant à leur regroupement ». Ibidem.

processus d'anonymisation des données personnelles[902]. Cette disposition irait dans le sens d'une certification des dispositifs d'anonymisation, comme nous l'avons envisagé précédemment[903], dans le cadre des dispositions visées à l'article 11 de la « LIL » de 1978 qui donnent comme mission à la CNIL d'assurer « la promotion » des technologies protectrices de la vie privée.

247. Modalités de mise en œuvre des missions de la CNIL.- L'étude de l'impact et de la nécessité de légiférer qui accompagne le projet LRN envisage trois possibilités pour garantir l'efficacité des prérogatives données à la Commission. Le projet de loi souhaite la création d'une instance *ad hoc* rattachée à la Commission Nationale de l'Informatique et des Libertés. Le projet de loi justifie par trois raisons le choix de la CNIL plutôt que du CNNum :

- de l'ancienneté de la commission et de la légitimité qu'elle a acquise avec le temps ;
- de son caractère d'autorité administrative indépendante, qui permettra de doter l'enceinte de réflexion des mêmes garanties d'indépendance ;
- des moyens dont dispose d'ores et déjà la commission[904].

La création d'une instance *ad hoc* se fonde sur les raisons qui ont mené à la création du Conseil Nation d'Ethique lors du vote de la loi bioéthique n°2004-800 du 6 août 2004[905].

248. Enfin, le projet de loi prévoit le recours à un instrument qui s'apparente à la demande d'autorisation préalable à la CNIL[906]. En effet, l'article 30 du projet de loi envisage la possibilité d'utiliser un « rescrit » en matière de traitement des données personnelles. Cet instrument, d'habitude utilisé en matière fiscale, permet d'indiquer la procédure à suivre dans d'une situation précise. Il a une valeur juridique protectrice vis-à-vis de l'administration. Dans le cas du traitement des données à caractère personnel, le rescrit délivré par la CNIL permettrait de délivrer un certificat de conformité attestant de la licéité du traitement. Si le recours au rescrit s'apparente à la demande d'autorisation préalable adressée à la CNIL, il permettrait néanmoins au responsable du traitement de

[902] Article 30, LRN n°3318, op. cit. loci.
[903] Cf *supra* Partie 2, Titre1, chapitre 1.
[904] Etude d'impact et de la nécessité de légiférer du projet de loi LNR n°3318, page 104.
[905] Loi n° 2004-800 du 6 août 2004 relative à la bioéthique, JORF 182.
[906] Cf supra. P101.

gagner en rapidité pour la mise en œuvre *conforme* du traitement. Il obligerait également le responsable à informer précisément la CNIL de la finalité du traitement car le rescrit ne serait opposable à la Commission que si le responsable du traitement avait fourni la totalité des informations à l'autorité. Quoi qu'il en soit, les garanties que nécessite l'organisation des plateformes numériques passe par l'augmentation des pouvoirs de l'Autorité Administrative Indépendante[907], même si le projet de LRN a pour objectif de promouvoir une nouvelle démocratie *numérique* fondée sur l'autonomie des personnes dans le « monde numérique ».

b) Le renforcement de la protection de la vie privée « en ligne »

249. Modification de la « LIL ».- Le projet de LRN prévoit la modification du chapitre V de la « LIL » de 1978 qui concerne les obligations du responsable du traitement. En effet, l'article 28 de la LRN prévoit d'imposer au responsable du traitement l'obligation de mettre à disposition de l'utilisateur, des moyens électroniques lui permettant d'exercer directement ses droits en ligne. En l'occurrence, le droit à l'information et le droit d'accès visés à l'article 32 de la loi «Informatique et Libertés». Le projet fait notamment référence au concept du « *privacy by design* » qui vise à promouvoir la mise en œuvre d'outils en ligne clairs et lisibles permettant d'accéder et de gérer les informations rapidement et de façon intelligible[908].

250. La portabilité et la récupération des données.- La récupération des données est une possibilité laissée à l'utilisateur de récupérer les données qu'il a lui-même déposées lors de l'utilisation de services en ligne tels que les mails, photos, historiques de navigation etc. Cette option permettrait de favoriser le droit des utilisateurs de choisir un nouveau fournisseur de services en ligne. Le CNNum indique que cette prérogative se justifie car, à l'heure actuelle, il « est fastidieux[909] » de procéder à la récupération des informations auprès des opérateurs. Le Conseil National Numérique constate que tout est mis en œuvre pour décourager les utilisateurs et les consommateurs de récupérer leurs informations. Le Conseil et le projet de LRN affirment que les solutions de stockage « en nuage » justifient cette nécessité de pouvoir disposer de ses informations. La portabilité des droits est jugée

[907] J.L Autin, « *Le devenir des Autorités Administratives Indépendantes* », RFDA 2010, page 875.
[908] Cf. supra, le droit à l'information p180.
[909] CNNum, Avis du 30 novembre 2015, disponible sur www.ccnumerique.fr.

comme essentielle par certains qui considèrent que la portabilité permettrait de développer le secteur économique des services de données « en permettant aux internautes de retrouver et d'interconnecter leurs données personnelles [910]». La portabilité des droits est un enjeu majeur en ce qui concerne les libertés individuelles. Ainsi, le projet de LRN affirme que la libre disposition des données à caractère personnel est, par nature, destinée à garantir l'effectivité des droits d'opposition et de rectification. Le projet de loi appuie son argumentation sur le principe de libre disposition de ses données personnelles affirmé par la Cour Constitutionnelle allemande en 1983. En effet, la Cour allemande indique que cette « liberté » permet à l'individu de disposer de son droit à « *l'autodétermination informationnelle »* qui confère « *le pouvoir de l'individu de décider lui-même […] quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui ».*

251. La modification de l'article 9 du Code civil.- L'inscription du droit à la portabilité des droits et du droit de disposer de ses données personnelles est une proposition du projet LRN. Cette inscription à l'article 9 du Code civil serait un moyen de rattacher la notion de données à caractère personnel à la notion de vie privée. Cette proposition du projet est inspirée de la solution dégagée par la Cour de Cassation le 10 septembre 2014. Dans cette décision, la Cour affirme, sur le fondement des articles 9 et 1382 du Code civil, que « *le choix d'une personne physique comme mot-clé destiné à faciliter le référencement par les moteurs de recherche sur internet des pages qui ne le supportent n'est pas fautif lorsqu'il n'est associé à aucune autre donnée personnelle, et ne le devient, le cas échéant, que lorsqu'est répréhensible le contenu de la page à laquelle le mot-clé est associé [911]».* Cependant, le projet de loi écarte cette possibilité aux motifs que cette disposition, sans être orientée vers la thèse patrimoniale, n'est pas la meilleure réponse « sauf pour les personnes d'une particulière richesse ou notoriété » car « la valeur des données personnelles d'un individu est très limitée, de l'ordre de quelques centimes d'euros ». En outre, l'étude de impact et de la nécessité de légiférer ajoute que :

> *« La reconnaissance du droit de propriété de l'individu sur ses données pourrait poser des difficultés juridiques pour les pouvoirs publics. Ainsi, par exemple, les limites apportées par la loi du 6 janvier 1978 concernant le traitement des données personnelles*

[910] E. Leandi, Fiche CCNum *La portabilité,* 2015, disponible sur www.ccnumerique.fr
[911] Cass. Civ. 1ère, 10 septembre 2014, n°13-12.464 (ECLI :FR :CCASS :2014 :C101002)

devraient être justifiées au regard de l'atteinte au droit de propriété en tenant compte des jurisprudences de la Cour Européenne des droits de l'homme et du Conseil Constitutionnel. Reconnaître un droit de propriété de l'individu impliquerait en réalité de renoncer largement à la logique de protection. »

Cette position met ainsi un terme au débat qui avait été lancé au sujet de la nécessité de reconnaître un droit de propriété aux personnes concernant leurs données personnelles[912]. Même si, lors de la rédaction du projet de LRN, la CNIL a affirmé[913] que la libre disposition des données personnelles permettrait un renforcement « positif de la capacité de l'individu de maîtriser l'usage de ses données », elle rappelle que ce principe est déjà proclamé à l'article 1[er] de la loi «Informatique et Libertés» de 1978 modifiée.

Ainsi, le projet de loi LRN affirme qu'une modification du chapitre II de la « LIL » de 1978 qui renforcerait les droits au regard de la finalité du traitement serait plus pertinent. Le projet de loi ajoute qu'il serait également « pertinent » de modifier le chapitre V de la « LIL » notamment en insérant à l'article 32 la durée de conservation en fonction des catégories de données traitées. Ces modifications permettraient un renforcement du droit à l'information, dont l'obligation qui incombe au responsable du traitement serait proportionnelle à la finalité du traitement[914].

***Conclusion*.-** Il semble, en effet, que l'insertion de nouvelles dispositions au sein de loi «Informatique et Libertés» de 1978 modifiée soit une solution pertinente, compte tenu, non seulement, du caractère indéniablement protecteur des droits et libertés attachés à la personne, mais, également, dans un souci de ne pas disperser des textes concernant la protection des données à caractère personnel.

En outre, il convient également de souligner que le projet de loi prévoit la modification de certaines dispositions du Code de la consommation qui ont déjà fait l'objet d'une abrogation. En effet, en matière de régulation et de loyauté des plateformes, le projet de « loi pour une République Numérique » prévoit la modification de l'article L. 111-5-1 du Code de la consommation qui a été abrogé par l'article 37 de l'ordonnance n°2016-301 du 14 mars 2016. Il n'en demeure pas moins que le projet de loi présente un potentiel certain de solutions qui permettront d'anticiper la transposition en droit interne du nouveau

---

[912] Thèse soutenue par l'auteur américain J. Lanier, cf Introduction, « vers une propriété des données personnelles ? ». « Who owns the future », Edition Simon & Schuster, 2013.
[913] Etude de l'impact et de la nécessité de légiférer op. cit. loci. Page 99.
[914] Article 26 et 27 du projet de LRN n°3318 op. cit. loci.

Règlement européen sur la protection et la circulation des données à caractère personnel au sein de l'Union Européenne[915]. Enfin, sans remettre en question l'existence et le pouvoir de régulation des AAI comme la CNIL, l'apport d'une régulation citoyenne *numérique* pourrait être complémentaire des missions d'information et de régulation des Autorités Administrative Indépendantes, notamment grâce à l'instauration du guichet unique permettant une centralisation des plaintes.

[915] Règlement du Parlement européen et du Conseil, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, du 27 avril 2016, n°2016-679, JOCE 119/1

Titre 2 : Le nouveau cadre juridique Européen

Il conviendra en premier lieu d'étudier le contenu du nouveau Règlement européen ainsi que les différentes propositions qui ont permis l'élaboration du nouveau texte afin d'effectuer une comparaison avec la directive 95/46/CE (Titre 1). Enfin, le texte règlementaire met en place un nouvel organe de contrôle qui jouera un rôle central en matière de protection des personnes. En effet, le Délégué à la Protection des Données remplacera l'actuel CIL et sera rattaché directement au responsable du traitement (Titre 2).

Chapitre 1 : Le nouveau Règlement européen pour la circulation des données personnelles

Sans alourdir les dispositions de la directive européenne de 1995 dont s'inspire le nouveau texte européen, le Règlement européen vient compléter et préciser certaines procédures en matière de traitement de données à caractère personnel. Il permet d'élargir le champ d'application de la protection y faisant figurer certaines données sensibles comme les données de santé. Le nouveau Règlement européen prévoit de nouveaux outils juridiques permettant un contrôle renforcé des informations par la personne concernée par le traitement et assure une effectivité des droits des personnes en consacrant un droit d'action collective (Section préliminaire). De plus, le nouveau Règlement européen renforce les obligations du responsable du traitement, notamment en matière de preuve de la recherche de consentement et d'information (Section 1). L'innovation remarquable du nouveau Règlement européen tient, en outre, à l'instauration d'un nouvel acteur en matière de protection des données à caractère personnel : le Délégué à la Protection des Données (DPD) qui fait l'objet d'une désignation obligatoire, dans certains cas, et dont il convient d'analyser les fonctions et le statut (section 2).

Section préliminaire : Présentation du Règlement et analyse comparée avec la directive 95/46/CE

La député au Parlement européen V. Reding[916] indiquait[917] qu'une étape importante devait être franchie dans le processus de réforme du cadre européen en matière de protection des données personnelles et de la vie privée, lors la proposition de règlement, publiée par la Commission le 25 janvier 2012. Cette proposition visait le futur cadre général européen en matière de protection des données à caractère personnel et a remplacer l'actuelle directive n° 95/46 de 1995. La commission des libertés civiles « LIBE » du

[916] En 2010 : vice-présidente et commissaire à la justice, aux droits fondamentaux et à la citoyenneté de la Commission Europénne.

[917] Extrait de son discours disponible sur http://europa.eu/rapid/press-release_IP-12-46_fr.htm?locale=fr

Parlement européen avait adopté un texte de compromis le 21 octobre 2013 qui comportait 104 amendements. Ce compromis a servi de base de réflexion pour l'adoption la résolution n°2013/2188 du Parlement dont l'objectif était de fixer le nouveau cadre européen de protection des données à caractère personnel et d'abroger l'actuelle directive n°95/46/CE. Le nouveau Règlement a été adopté le 27 avril 2016 et publié le 4 mai 2016 après quatre années de négociations entre la Commission et le Parlement européen. Le nouveau Règlement comprend 92 articles et sera directement applicable à l'ensemble des Etats membres à compter de 2018.

Le nouveau cadre européen de la protection des données à caractère personnel tend vers deux évolutions importantes, d'ordre technique, en matière de traitement des données à caractère personnel. Une présentation générale de l'évolution du projet permettra de prendre la mesure de l'importante réforme qui devra être effective d'ici deux ans.

252. L'apport de la définition de données pseudonymes.- La notion de « données pseudonymes », issue du rapport Albrecht[918], introduit la notion de données personnelles qui peuvent être attribuées à une personne en particulier, en ayant recours à des « informations complémentaires, du moment que de telles informations » sont « conservées séparément et font l'objet de mesures techniques et organisationnelles pour permettre leur non-attribution ». D'après le texte de compromis, les « données anonymes » sont des « données personnelles collectées, altérées, ou traitées de quelque façon que ce soit, de manière à ne plus pouvoir être attribuées à une personne concernée », qui « ne doivent pas être considérées comme des données personnelles » et sont donc exclues du champ d'application du règlement. En ce qui concerne les « données chiffrées », il s'agit de « données personnelles qui, par des mesures de protection technique, sont rendues inintelligibles à toute personne qui n'est pas autorisée à y accéder ». Or, l'objectif des « données pseudonymes » était, selon le député vert allemand, « d'alléger[919] » la procédure du responsable de traitement qui n'était pas tenu de respecter les obligations d'information de la personne concernée par le traitement de ses données à caractère personnel. Cependant, à la lecture de l'article 11 du nouveau Règlement, on relève que « le

[918] Député vert Allemand qui désignait « un identifiant unique qui est spécifique à un contexte donné et qui ne permet pas l'identification directe d'une personne physique mais permet de distinguer une personne concernée ».

[919] Voir le rapport Albrecht sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, page 30, disponible sur http://www.europarl.europa.eu.

responsable du traitement n'est pas tenu d'obtenir des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter une disposition du présent règlement ». Ainsi, l'article 4 §5 du nouveau Règlement définit la «pseudonymisation» comme étant « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

253. L'intégration des nouvelles pratiques liées au « profilage ».- L'usage du « profilage » est un élément central de la réforme : l'article 22 du nouveau Règlement confère à la personne concernée un droit d'opposition. Il reprend l'article 14 de la directive 95/46/CE auquel il apporte des précisions, notamment en ce qui concerne la charge de la preuve et son application au marketing direct. Ce droit d'opposition au profilage se définit comme une « mesure produisant des effets juridiques à son égard ou l'affectant de manière significative sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects personnels propres à cette personne physique ou à analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement[920] ».
En 2013, le texte de compromis de la Commission LIBE se penchait notamment sur les possibilités de l'utilisation du profilage, en proposant qu'il soit utilisé dans trois cas : lorsque la loi le prévoit, s'il est nécessaire à la conclusion ou à l'exécution d'un contrat et si le consentement de la personne a été dûment recueilli. En d'autres termes, le profilage devait être mis en place dans le respect des libertés fondamentales et ne devait pas aboutir à une discrimination résultant de l'utilisation des données listées à l'article 20 et à l'article 9 du projet de Règlement européen. Ainsi, l'article 22 du nouveau Règlement de 2016 reprend la proposition du Règlement en définissant le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser » de telles données « pour évaluer certains aspects personnels relatifs à une personne [...] notamment pour analyser ou prédire [921]» des préférences ou des comportements de ladite personne. Le

[920] Article 20 du projet de règlement relatif au traitement des données à caractère personnel.
[921] Article 4 §4 du Règlement

nouveau Règlement accorde à la personne, sur ce fondement, un droit d'opposition qui tient compte des nouvelles pratiques prédictives.

L'article 11 §2 du projet de Règlement vise la « standardisation de l'information des personnes » du projet européen et prévoit que « le responsable du traitement applique des règles internes transparentes et facilement accessibles en ce qui concerne le traitement des données à caractère personnel et en vue de l'exercice de leurs droits par les personnes concernées. »

La commission LIBE a complété le projet européen en ajoutant « la nécessité de fournir cette information sous format d'icônes tout en réservant à la Commission européenne le pouvoir de définir leur contenu par la voie d'actes délégués »[922]. L'objectif de la Commission est de rendre complètement accessibles et compréhensibles les documents d'information et les conditions de traitement des données grâce à l'intégration d'icônes permettant de savoir qui pourra accéder aux informations[923]. La commission LIBE indiquait également que le responsable du traitement devrait faire figurer un certain nombre d'icones clairs permettant de connaître la finalité de chaque information recueillie ainsi que de son éventuelle conservation ou partage avec des tiers. Par exemple, lors du remplissage d'un formulaire, nous pouvons imaginer qu'à côté de la ligne où la personne devra renseigner son nom, un icône fera apparaître un message qui lui permettra d'identifier toutes les personnes qui auront accès à ce renseignement. C'est ce que prévoit l'obligation d'information « normalisée » du nouveau Règlement de 2016[924].

254. La définition des données de santé.- Le nouveau Règlement européen prévoit désormais que le régime de protection s'applique lorsqu'il s'agit de « données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne[925] ».

Le considérant n°35 précise que les données de santé comprennent « toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne

---

[922] *Réforme du cadre européen de la protection des données à caractère personnel : où en est-on* ?, N. Métallinos et N. Botchorichvili, Avocate Bird & Bird, Revue Lamy Droit de l'Immatériel, 2013 page 99.

[923] Cf Document de la Commission LIBE, la normalisation visuelle, annexe n°2.

[924] *Ibid*.

[925] Article 4 §15 du Règlement

concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro ».

Le Règlement définit aussi les données « relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé [926]» et les données biométriques « résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique[927] ».

255. Le renforcement du consentement.- Que cela soit en matière de droit commun ou dans le domaine médical, la proposition de la commission LIBE présentait, déjà en 2013, une solution permettant un cadre « viable[928] » de protection des données à caractère personnel. La Commission prévoyait une gestion personnelle des données par l'utilisateur, mais aussi par le patient dans le cadre d'un déploiement du DMP transfrontalier. Ainsi, le Règlement européen consacre quatre paragraphes aux conditions de consentement à l'article 7 :

> *« 1. La charge de prouver que la personne concernée a consenti au traitement de ses données à caractère personnel à des fins déterminées incombe au responsable du traitement.*
>
> *2. Si le consentement de la personne concernée est requis dans le contexte d'une déclaration écrite qui concerne également une autre affaire, l'exigence du consentement doit apparaître sous une forme qui le distingue de cette autre affaire.*
>
> *3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement préalablement donné.*
>
> *4. Le consentement ne constitue pas un fondement juridique valable pour le traitement lorsqu'il existe un déséquilibre significatif entre la personne concernée et le responsable du traitement. »*

[926] Article 4 §13 du nouveau Règlement op. cit loci
[927] Article 4 §14 du nouveau Règlement op. cit loci
[928] Considérant 161 du nouveau Règlement op. cit. loci.

La lecture comparative de la directive européenne n°95/46/CE du 24 octobre 1995 et du nouveau Règlement européen montre que l'on passe d'un consentement « exprès[929]» donné par la personne concernée par le traitement, à un responsable qui se voit dans l'obligation de prouver que le consentement à été exprimé par l'individu.

256. Un consentement distinct de tout autre document.- Le consentement de la personne concernée par le traitement de ses informations doit apparaître sous une forme distincte de tous les autres documents[930]. Les propositions de la Commission LIBE ont été adoptées par le Parlement européen dans la résolution du 12 mars 2014 et sont prévues en bonne place à l'article 7 du nouveau Règlement européen de 2016.

Dans le domaine médical, et, plus précisément, en matière de la télésanté, les nouvelles Technologies de l'Information et de la Communication (TIC) présentent un enjeu déterminant en la matière. Dans le domaine du développement de ces outils, l'UE a mis en place un plan d'action en 2004, dans lequel elle reconnaît explicitement que les TIC jouent un rôle clé dans le domaine de la santé et que la nouvelle technologie « joue, sans conteste, un rôle important dans la stratégie eEurope de l'Union Européenne et elle est indispensable pour doper la croissance et créer des emplois hautement qualifiés dans une économie dynamique et fondée sur la connaissance [931]». Elle ajoute qu'il s'agit de « répondre à l'augmentation de la demande de services de santé et de […] réduire les inégalités en matière d'accès à des soins de santé de qualité ; répondre à la mobilité croissante des patients et des professionnels de santé dans le marché intérieur ». La télésanté est également l'objet de toutes les attentions dans le programme i2010 qui vise à mettre en avant les projets nouveaux permettant de développer les TIC. La commission, dans son plan d'action, se focalise notamment sur la mise en place de soins de santé personnalisés et durables au service des patients et des professionnels de santé tels que : les systèmes de contrôle à distance du statut médical, les matériels portables de diagnostic ou les outils électroniques capables d'effectuer une prescription personnalisée. Cela pose donc la question du traitement des données de santé à caractère personnel.

---

[929] Article n°7 a) de la directive n°95/46/CE 24 octobre 1995.

[930] Article 7 § 2 du Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

[931] Commission européenne, Communication au Conseil, au Parlement européen, au Conseil économique et social européen et au Comité des régions, Santé en ligne - Améliorer les soins de santé pour les citoyens européens : plan d'action pour un espace européen de la santé en ligne, COM(2004)356final.

Le dernier plan d'action « 2012-2020 » de la Commission souligne que « maintenant, plus que jamais, les gens surveillent leur santé et leur bien-être en ligne ou par des dispositifs tels que les Smartphones. Le plan d'action reflète ce changement de comportement et vise à renforcer la confiance des utilisateurs dans ces outils numériques et des applications, tout en s'assurant que les conditions du marché encouragent l'innovation continue.[932]»

Il semble donc que le développement de la santé connectée soit une réelle préoccupation à l'échelle européenne. La nouvelle définition du cadre juridique européen des prestations de télésanté permettra d'en établir les règles de fonctionnement en termes de traitement des données de santé à caractère personnel qui seront traitées via les TIC. L'usage des TIC se coordonne parfaitement avec le projet de révision de la directive n°95/46/CE du 24 octobre 1995.

257. La reconnaissance d'une action collective.- On peut remarquer l'introduction du recours juridictionnel simplifié en cas de traitement illicite. L'article 76 du projet de Règlement prévoit la possibilité de saisir une juridiction au nom d'une ou plusieurs personnes concernées par un traitement illicite. Ce recours est issu de la « class action », procédure anglo-saxonne qui permet à un groupe de personnes ayant un intérêt commun de se regrouper dans une action commune pour faire valoir leur droit ou indemniser leur préjudice[933].

258. Les prérogatives de la Commission en matière de transfert.- En matière de traitement de données à caractère personnel transmises à un pays tiers, le projet de Règlement européen[934] prévoyait aux articles 40 et suivants que les entreprises qui n'ont ni serveurs, ni établissements dans le territoire de l'Union Européenne seraient soumises au cadre européen relatif à la protection des données personnelles, dès lors qu'elles proposeraient des biens ou services aux citoyens européens. Ainsi, Le nouveau Règlement vise l'obligation pour les entreprises de revoir leurs méthodes de traitement pour être conformes aux nouveaux standards européens. Cette préoccupation des échanges de données vers des pays tiers provient vraisemblablement de l'accord sur la santé en ligne signé par Mme N. Kroes, vice-présidente de la Commission européenne, et Mme K. Sebelius, secrétaire américaine à la santé et aux affaires sociales. Cet accord vise à

[932] Traduit de l'Anglais *: European Commission*, Memo, Brussels, 7 Décembre 2012.
[933] Définition lexique juridique Dalloz.
[934] Projet de règlement européen relatif à la protection des personnes physiques à l'égard des traitements des données à caractère personnel.

promouvoir une approche commune sur l'interopérabilité des dossiers médicaux électroniques et à dynamiser « le potentiel de ce marché pour les entreprises de l'UE qui souhaitent exercer des activités aux États-Unis et inversement[935] ». Il faut retenir que, de manière générale, tous les Etats membres doivent limiter - sur le fondement du principe de finalité légitime du traitement - « le partage d'informations à ce qui est nécessaire pour la réalisation par chacun de ses propres fonctions, et, enfin, un partage de l'information entre les professionnels liés par le secret professionnel ». Ces règles concernent les traitements qui sont effectués au sein de l'UE. Pour le cas où les données doivent faire l'objet d'un transfert vers un pays tiers, la directive de 1995 prévoit que chaque Etat membre peut autoriser ce transfert si l'Etat destinataire dispose des garanties suffisantes de sécurité et de confidentialité concernant l'échange de données sensibles à caractère personnel[936].

259. Le nouveau Règlement prévoit que, dans un objectif de « plein respect » du Règlement, il revient à la Commission européenne de définir si un « pays tiers offre un niveau de protection adéquat ». Les articles 44 à 48 du nouveau Règlement confèrent à la Commission européenne le pouvoir de décider si un pays tiers « assure » ou n'assure plus un niveau de protection adéquat des données. La rédaction du nouveau Règlement est sans équivoque et prévoit que :

> *« La Commission, après avoir évalué le caractère adéquat du niveau de protection, peut décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, assure un niveau de protection adéquat au sens du paragraphe 2 du présent article. L'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale. L'acte d'exécution précise son champ d'application territorial et sectoriel et, le cas échéant, nomme la ou des autorités de contrôle visées au paragraphe 2, point b), du présent article. L'acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2. [937]»*

[935] Extrait du communiqué de presse de N. Kroes op. cit.
[936] Article 25 de la directive n°95/46/CE du 24 octobre 1995 op. cit. loci.
[937] Article 44 §2 du Règlement européen.

Certains[938] interprètent cette disposition comme une *réaction* à l'arrêt de la CJUE du 6 octobre 2015[939] dans lequel la Cour de Justice invalide la décision de la Commission européenne qui avait autorisé le transfert de données à caractère personnel vers un pays tiers[940]. Cette extension du champ territorial des règles européennes, c'est-à-dire le fait que le nouveau texte européen s'applique également aux traitements de données depuis un pays tiers vers l'Union Européenne, permet, notamment, la mise en place du guichet unique. Ainsi, le responsable du traitement ne devra s'adresser qu'à une seule autorité au sein de l'Union européenne.

Enfin, les « CNIL » visées aux articles 51 à 58 du nouveau Règlement seront dotées d'un plus grand pouvoir de sanction pécuniaire. En effet, celles-ci pourront prononcer une sanction allant jusqu'à 20 000 000 d'euros ou 4% du chiffre d'affaire annuel de l'entreprise. Le nouveau cadre européen constitue une véritable révolution[941] compte tenu des nouvelles obligations en matière de traitement des données à caractère personnel.

Section 1 : Les nouvelles obligations du responsable du traitement

Le nouveau règlement européen met en place une nouvelle dynamique en ce qui concerne les obligations générales du responsable du traitement (a). En effet, le Règlement renforce les obligations du responsable du traitement notamment en matière de sécurité (b).

a) Les obligations générales

260. La suppression des déclarations préalables.- Le Règlement européen du 14 avril 2016 ne subordonne plus la mise en œuvre du traitement à l'accomplissement de formalités préalables telles que les demandes d'autorisations. En contre-partie, le Règlement impose au responsable du traitement de se conformer à toutes les mesures

---

[938] E. Derieux, « *Protection des données à caractère personnel et activités de communication publique Apports du règlement européen du 27 avril 2016 au regard de la précédente directive du 24 octobre 1995 et de la loi française du 6 janvier 1978 (révisée par celle du 6 août 2004)* », RDLI, 2016 n°128.

[939] CJUE, affaire n° C-362/14, Maximillian Schrems c Data Protection Commissioner, du 6 octobre 2015.

[940] Padova Y., Le *Safe Harbor* est invalide. Et après ? Analyse des fondements de l'arrêt de la CJUE et de ses conséquences, RLDI 2015/120, n° 3867, p. 50-64.

[941] L. Marino, « *Le règlement européen sur la protection des données personnelles: une révolution!* », La Semaine Juridique Edition Générale n° 22, 30 Mai 2016, p 628.

techniques et organisationnelles en fonction des enjeux que représentent le traitement de certaines données. Le considérant 51 du Règlement affirme que « les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits ».

261. La Protection des données dès la conception et par défaut.- L'article 25 du Règlement prévoit que le responsable du traitement doit se conformer aux mesures techniques et organisationnelles nécessaires afin de garantir « par défaut » la protection des données à caractère personnel. Le Règlement impose ainsi au responsable, quel que soit le traitement, de mettre en œuvre toutes les mesures de protection et de sécurité tant « au moment de la détermination des moyens de mise en œuvre du traitement [942]» qu' « au moment du traitement lui-même[943] ». Le principe de protection par défaut implique que le responsable du traitement doit respecter le principe de minimisation des données et mentionner la durée de conservation de ces données, avant même la mise œuvre du traitement. Le principe de minimisation par défaut implique de définir clairement la finalité afin que ne soient collectées *seulement* les données absolument nécessaires à la réalisation de la finalité. Cette obligation pourrait paraître quelque peu redondante avec la législation déjà en vigueur qui impose au responsable du traitement de définir clairement la finalité du traitement envisagé. Cependant, l'innovation notable du Règlement tient à l'obligation d'identifier les traitements à risques, notamment avec l'obligation de « l'étude d'impact[944] » dont les lignes directrices avaient été dégagées par le G29[945].

262. Les critères d'identification des traitements.- La section 3 du Règlement est consacrée à la mise en œuvre des critères permettant d'identifier les traitements à risque. Le texte européen reprend le considérant 53 de la directive 95/46/CE de 1995 visant les critères relatifs à la nature, la portée et la finalité du traitement. Le Règlement européen ne mentionne pas que l'étude d'impact s'apparente à une formalité préalable. En effet, cette étude permet, en réalité, d'obliger le responsable du traitement à évaluer le niveau de sécurité et de mise œuvre des garanties de protection des données à caractère personnel lors du traitement. Selon le traitement envisagé, le responsable devra, par défaut, consulter

[942] Article 25 alinéa 1er du Règlement européen du C-2016/679 op. cit. loci.
[943] Ibidem.
[944] Ibidem. Article 35.
[945] Etude d'impact des données, G29,WP 216 op. cit. loci.

l'autorité de contrôle compétente en fonction des données à traiter, ou le Délégué à la Protection des Données (DPD) si le traitement comporte des données « à risques [946]». Le §3 de l'article 35 mentionne la liste des traitements nécessitant une étude d'impact :

« a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;
b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10;
c) la surveillance systématique à grande échelle d'une zone accessible au public. »

Néanmoins, le responsable du traitement devra effectuer une analyse d'impact plus précise si le traitement envisagé entre dans la liste publiée par le comité visé à l'article 58 du Règlement. L'analyse d'impact devra ainsi comporter :

« a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;
b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;
c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1;
d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées. »

263. Les mesures techniques.- Dans son avis concernant l'étude d'impact du traitement des données à caractère personnel, le G29 indique, dans la section consacrée à l'analyse technique, qu'un traitement de données à caractère personnel est considéré comme « fiable » dès lors que le traitement permet de résister à : « *l'individualisation*, qui

[946] Considérant n°77 du nouveau Règlement op. cit. loci.

correspond à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données ; à *la corrélation,* qui consiste dans la capacité de relier entre elles, au moins, deux enregistrements se rapportant à la même personne concernée ou à un groupe de personnes concernées (soit dans la même base de données, soit dans deux bases de données différentes). Si une attaque permet d'établir (par exemple, au moyen d'une analyse de corrélation) que deux enregistrements correspondent à un même groupe d'individus, mais ne permet pas d'isoler des individus au sein de ce groupe, la technique résiste à l'«individualisation», mais non à la corrélation; et enfin, à *l'inférence*, qui est la possibilité de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs.[947] » Le groupe de travail ajoute que si les solutions mises en place lors du traitement permettent de résister à ces « trois risques [le traitement] offrirait, par conséquent, une protection fiable contre les tentatives de ré-identification utilisant les moyens les plus susceptibles d'être raisonnablement mis en œuvre par le responsable du traitement des données ou par des tiers ».

264. En outre[948], le groupe de travail préconise plusieurs techniques permettant de garantir un traitement des données respectant toutes les conditions de sécurité et de confidentialité. Le G29 consacre une partie entière à la « pseudonymisation ». Le choix du G29 se justifie par le fait que cette technique est visée par le Règlement européen et qu'elle

[947] G29, avis, « Les techniques d'anonymisation » adopté le 10 avril 2014, page 13.

[948] L'avis adopté par le Groupe de travail reprend également toutes les mesures techniques qui permettent de garantir la sécurité et la confidentialité des données lors du traitement telles que : La randomisation qui « est une famille de techniques qui altèrent la véracité des données afin d'affaiblir le lien entre les données et l'individu. Si les données sont suffisamment incertaines, elles ne peuvent plus être rattachées à un individu en particulier. En elle-même, la randomisation ne réduira pas la singularité de chaque enregistrement, qui sera toujours dérivé d'une seule personne concernée, mais elle peut apporter une protection contre les attaques/risques relevant de l'inférence et peut être combinée avec des techniques de généralisation pour offrir de meilleures garanties de respect de la vie privée. Des techniques supplémentaires peuvent se révéler nécessaires pour empêcher qu'un enregistrement permette d'identifier un individu ». Ou bien encore la confidentialité différentielle qui présente les « avantages d'une approche reposant sur la confidentialité différentielle tient au fait que des ensembles de données sont communiqués à des tiers autorisés en réponse à une demande spécifique, plutôt que d'être publiés sous la forme d'un unique ensemble de données. Pour faciliter le contrôle, le responsable du traitement des données peut conserver une liste de toutes les demandes et requêtes afin de vérifier que les tiers n'ont pas accès à des données pour lesquelles ils ne disposent pas d'autorisation. Une requête peut aussi être soumise à des techniques d'anonymisation, incluant l'ajout de bruit ou la substitution, pour mieux garantir la confidentialité. Les recherches se poursuivent en vue de trouver un bon mécanisme interactif de question-réponse, qui soit capable tout à la fois de répondre assez précisément à n'importe quelle question (c'est-à-dire en ajoutant le moins de bruit possible) et de préserver la confidentialité », avis G29, op. cit. loci. Pages 15 à 22.

consiste à remplacer un attribut[949] (généralement un attribut unique) par un autre, dans un enregistrement. La personne physique est donc « toujours susceptible d'être identifiée indirectement ; par conséquent, la pseudonymisation ne permet pas, à elle seule, de produire un ensemble de données anonymes ». Cette technique est mise en avant par le groupe de travail car elle permet d'éviter une mise « en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée [950]». La technique de pseudonymisation permet l'utilisation de fonctions telles qu'une clé cryptée dont le décryptage ne serait possible qu'à condition de connaître la clé, et cette clé serait complétée par une fonction de « hachage [951]» qui ne pourrait pas être inversée. Cette fonction est elle-même complétée par un « salage », c'est-à-dire une valeur aléatoire ajoutée à l'attribut qui entraîne une réduction de la possibilité de découvrir la valeur d'entrée par recoupement. Cette technique a été approuvée et est utilisée par la CNIL en ce qui concerne l'anonymisation « à bref délai [952]».

265. La portée et la finalité de l'étude d'impact.- L'objectif de l'obligation du responsable du traitement de dresser une étude d'impact est de permettre, dans un premier temps, de garantir la conformité du traitement et, dans un second temps, d'identifier les traitements qui comportent des risques (même résiduels[953]) de ré-identification ou d'atteintes aux droits et aux libertés. Comme le fait remarquer le groupe de travail, il s'agit, enfin, que les responsables du traitement des données aient conscience qu'un ensemble de données anonymisées peut encore présenter des risques résiduels pour les personnes concernées[954]. Le considérant 71 du texte de compromis permet de se rendre compte que l'analyse d'impact est au cœur de la mise en place du traitement des données : « les analyses d'impacts sont l'essence même de tout cadre viable de protection des données. Elles garantissent que les entreprises soient conscientes dès le départ de toutes les conséquences possibles de leurs traitements. […] elles permettent de limiter le risque de violation des données ou de traitements portant atteinte à la vie privée […] tout au long de

[949] Un ensemble de données se compose des différents enregistrements relatifs à des individus (les personnes concernées). Chaque enregistrement se rapporte à une personne concernée et comporte une série de valeurs (ou « entrées ») pour chaque attribut (par exemple, l'année).
[950] Avis G29 op. cit. loci.
[951] Sur toutes les techniques de hachage voir aussi : Fonction de hachage par clé enregistrée, chiffrement déterministe ou fonction de hachage par clé avec suppression de la clé, Tokenization. Avis G29 op. cit. loci, page 23.
[952] Cf supra
[953] Voir introduction avis G29.
[954] Ibidem ; considérant 71 et suivants du Règlement européen .

leur cycle de vie, depuis la collecte jusqu'au traitement et à l'effacement des données, en décrivant, en détails, les traitements envisagés […] et les mesures pour réduire ces risques ».
Enfin, l'obligation d'effectuer l'étude d'impact incombe tant au responsable du traitement qu'à son sous-traitant.

266. La procédure de consultation préalable.- La procédure de consultation préalable visée par le Règlement européen reprend les dispositions de la directive 95/46/CE qui visent à limiter les possibilités de traitement grâce à un examen préalable. Cet examen est effectué lorsque l'analyse d'impact comporte un résultat démontrant que le traitement comporte des risques, même résiduels, concernant la protection des données. En d'autres termes, l'étude démontre que les moyens techniques de traitement ne permettent pas de neutraliser tous les risques et que des démarches supplémentaires sont à envisager. Cette procédure a pour but de garantir la conformité du traitement des données à caractère personnel et, surtout, d'essayer de réduire au maximum les risques de failles. Il convient de relever que cette procédure n'est en rien une procédure d'autorisation ; il s'agit d'une évaluation permettant au comité visé à l'article 58 du Règlement d'émettre un avis assorti d'une mention favorable ou de réserve. On peut difficilement penser qu'un responsable du traitement ne tienne pas compte de l'avis émis, compte tenu des nouvelles sanctions prévues[955].

b) Les obligations de sécurité

267. La fin de l'immunité du sous-traitant.- Le principal apport du Règlement est de mettre fin à une sorte d'immunité des sous-traitants sous l'empire de l'ancienne directive de 1995. En effet, le Règlement[956] prévoit un régime spécial de responsabilité du sous traitant. Le Règlement européen considère que la protection des droits et des libertés des personnes concernées, de même que la responsabilité des responsables et de leurs sous-traitants, demande une répartition claire des responsabilités, même lorsque la finalité du traitement a été déterminée conjointement avec d'autres responsables ou sous-traitants. Il appartient cependant au responsable du traitement et au sous traitant de définir leurs rôles respectifs dans l'accomplissement de leurs missions, dans le respect des exigences définies

[955] Cf supra, « Les nouvelles sanctions prévues » p 241.
[956] Article n°24 et suivants du Règlement européen op. cit. loci.

par le Règlement. Cependant, le Règlement dispose que les deux parties liées au contrat ont un devoir d'assistance l'une envers l'autre et qu'il doit être mentionné au contrat[957].

268. L'obligation de sécurité et de confidentialité.- L'obligation de sécurité du Règlement européen reprend les dispositions des articles 16 et 17 de la directive de 1995 et complète cette obligation avec l'impératif de tenir compte des résultats obtenus par l'étude d'impact. Le Règlement impose de mettre en place une politique de sécurité obligeant le responsable du traitement « à tester, à analyser et évaluer régulièrement l'efficacité des politiques, des procédures et des plans de sécurité mis en place pour assurer une efficacité constante[958] ». De plus, l'obligation de sécurité contenue dans le Règlement impose tant au responsable qu'au sous-traitant de notifier les cas de violations de sécurité. Cette obligation est visée par l'article 33 du Règlement qui reprend les dispositions du règlement 611/2013 « concernant les mesures relatives à la notification des violations de données à caractère personnel », et remplace le délai de 24h initialement prévu par l'obligation de notifier les violations de sécurité dans les « meilleurs délais ». Si ce délai peut laisser penser que le responsable du traitement et le sous-traitant peuvent bénéficier d'une certaine souplesse, le Règlement impose néanmoins de mentionner un certain nombre d'éléments devant figurer dans la notification qui doit :

> *« a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;*
> *b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;*
> *c) décrire les conséquences probables de la violation de données à caractère personnel;*
> *d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. »*

Enfin, les paragraphes 4 et 5 de l'article 33 imposent que « si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent

[957] Ibidem, et voir le considérant n°171 du Règlement op. cit. loci.
[958] Article 30 §1 du Règlement européen op. cit. loci.

être communiquées de manière échelonnée sans autre retard indu » et « le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article. »
Cette obligation de notifications détaillées est cohérente avec la mise en place d'une obligation d'information renforcée visée aux articles 12 et suivants du Règlement européen.

Section 2 : L'obligation d'information renforcée

269. Le droit d'être informé.- Les articles 13 et 14 du Règlement prévoient que les personnes concernées par le traitement ont le droit d'être informées des informations détenues par le responsable du traitement et ceci sans frais. Le même article regroupe le droit d'opposition, de rectification et d'effacement. Si le Règlement prévoit que le droit d'opposition, de rectification et d'effacement soient regroupés sous le droit à être informé, c'est dans le but de faire peser cette obligation à la charge de l'exploitant des données personnelles. Ainsi, la formulation du considérant 58 est sans équivoque : « Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels[959]. »

270. Une information « intelligible ».- Le règlement européen prévoit des modalités différentes d'information seulement en ce qui concerne les exceptions à l'obligation d'information. Le Règlement différencie clairement les obligations du responsable du traitement, selon que les données sont collectées directement ou indirectement auprès de la personne concernée, les articles 13 et 14 prévoient que le responsable du traitement devra fournir dans les deux cas:

[959] Afin de comprendre ce que la notion de visuel recouvre, voir annexe n°2.

« a) L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement;

b) le cas échéant, les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) les catégories de données à caractère personnel concernées;

e) le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel;

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition »

Le responsable du traitement est également tenu de fournir des informations supplémentaires permettant de garantir « un traitement équitable et transparent ». En effet, le §2 de l'article 14 prévoit, en plus et de manière obligatoire, d'indiquer à la personne concernée par le traitement, la durée de conservation de ses données à caractère personnel, et si la durée n'est pas déterminée, le responsable devra indiquer les « critères utilisés » pour déterminer celle-ci[960]. Il devra motiver et prouver l'intérêt légitime du traitement sur le fondement de l'article 6 (licéité) du Règlement. Il devra également fonder l'intérêt légitime du traitement lorsqu'il est effectué par des tiers[961] et informer la personne concernée de l'existence du droit de « demander au responsable » l'accès aux données, la rectification ou l'effacement ainsi que le droit de s'opposer au traitement. Il convient d'ajouter que l'article 14 impose au responsable du traitement d'informer la personne de son droit à *retirer* ses données personnelles en lui permettant de les faire stocker par un autre exploitant et en lui notifiant sont droit « à la portabilité des données [962]».

271. Une information loyale et complète.- Le Règlement impose, au §2 d) de l'article 13 et 14, que le responsable du traitement doit permettre à la personne concernée de « retirer son consentement » sans que ce retrait ne porte atteinte à la licéité du

[960] Article 14 §2 a), du Règlement C-2016/679 op. cit. loci.
[961] Article 14 §2 b), du Règlement C-2016/679 op. cit. loci.
[962] Ibidem.

traitement. Il ressort de cette disposition que le consentement n'est pas un pendant du droit d'opposition mais une prérogative que l'on peut qualifier *d'autonome,* au même titre que le droit au déréférencement[963]. Il convient de recouper ce droit de « retrait du consentement » avec le considérant 67 du Règlement qui indique que la personne concernée devrait avoir le droit de rendre, « même de façon temporaire », indisponibles les données qui font l'objet d'un traitement, en tenant compte de la nature de ces données[964].

De même, le responsable du traitement a l'obligation de fournir la source dont sont issues les données à caractère personnel. Si le responsable n'est pas en mesure d'en déterminer l'origine, il doit en indiquer le *degré* de confidentialité, c'est-à-dire qu'il devra indiquer à la personne si ses données sont publiques ou non[965]. Enfin, le responsable du traitement devra fournir à la personne concernée par le traitement, les informations qui ont servi à la prise d'une décision automatisée, et, surtout, l'avertir des conséquences de cette décision[966]. Ainsi, le responsable du traitement devra indiquer à la personne concernée son droit d'introduire une réclamation auprès d'une autorité compétente[967].

On constate que les informations qui doivent être fournies à la personne sont plus nombreuses que celles initialement prévues par la directive de 1995. En réalité, là où la directive 95/46/CE prévoyait la fourniture d'informations complémentaires en raison des circonstances particulières, le Règlement prévoit la fourniture d'une information complémentaire quelle que soit la nature du traitement.

272. La fourniture d'une information normalisée.- Le considérant n°60 fait référence aux nouvelles exigences de transparence et de loyauté en indiquant que cette nécessité passe par une information « accompagnée d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu ». C'est également ce que préconisait la Commission LIBE lors des débats concernant l'élaboration du projet de Règlement le 12 mars 2014[968]. La fourniture *normalisée* passe par l'utilisation de pictogrammes informant la personne concernée -selon le principe de minimisation- de la finalité du traitement, des cessions ou ventes des

[963] Cf supra le droit à l'oubli et au déréférencement.
[964] Articles 6 et 9 du Règlement C-2016/679 op. cit. loci.
[965] Articles 14 §2 f), du Règlement C-2016/679 op. cit. loci.
[966] Articles 13 et 14 f) du Règlement C-2016/679 op. cit. loci.
[967] Articles 13 et 14 e) du Règlement C-2016/679 op. cit. loci.
[968] Résolution législative du Parlement européen du 12 mars 2014, sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, amendement 109.

données à des tiers et enfin le cryptage des informations pendant la durée de conservation[969].

273. Le moment de la fourniture de l'information.- L'article 12 §3 du Règlement européen prévoit que le responsable du traitement doit fournir, dans un délai d'un mois, les informations qui ont fait l'objet d'une demande par la personne concernée. Le texte européen précise que ce délai peut être prolongé de deux mois lorsque le responsable démontre la complexité de la demande formulée par la personne. Enfin, le responsable doit fournir les informations visées au §1 des articles 13 et 14 du Règlement et lorsqu'il aura obtenu les données, de façon directe ou indirecte, il devra alors fournir les compléments d'information prévus aux §2 des articles 13 et 14. En d'autres termes, les dispositions du Règlement laissent une marge de manœuvre au responsable du traitement qui ne peut s'expliquer que pour des raisons techniques, il paraît, en effet, plus *logique* que l'information soit délivrée à partir du moment où les données seront collectées. Le Règlement prend en compte les difficultés techniques et les couts de mise en œuvre du traitement afin d'éviter une dépense supplémentaire inutile au responsable du traitement qui informerait une personne qui n'aurait pas délivré la totalité des données nécessaires à la réalisation de la finalité.

274. Dérogations.- Le nouveau Règlement reprend les dérogations déjà prévues par l'ancienne directive de 1995. En effet, le Règlement autorise le responsable du traitement à ne pas informer la personne concernée si elle a été déjà avisée de la collecte et du traitement de ses données. C'est le cas de l'information préalable au traitement, visée à l'article 13 de la directive 95/46/CE du 26 octobre 1995. Cette dérogation est autorisée principalement dans le cadre de la sécurité d'Etat, à des fins archivistiques ou à des fins historiques et de recherches, dans le cas où l'Etat membre prévoit expressément l'enregistrement ou la communication de telles données[970]. Enfin, lors des débats portant sur la mise en place du projet de Règlement, l'amendement 110[971] prévoyait que l'information de la personne concernée n'était délivrée, dans les micros entreprises, que lorsque celle-ci en avait fait la demande (article 14 ancien). La dernière version de 2016 du Règlement justifie la suppression de cet allégement dans le considérant n°167 en indiquant

[969] Article 12 § 7 du Règlement C-2016/679 op. cit. loci.
[970] Article 23 §1 et §2 du Règlement C-2016/679 op. cit. loci.
[971] Résolution du Parlement européen op. cit. loci.

qu'afin « d'assurer des conditions uniformes d'exécution du présent règlement », le Règlement confère à la Commission le pouvoir « d'envisager des mesures spécifiques pour les micros, petites et moyennes entreprises ». Ce pouvoir est prévu à l'article 40 du Règlement et dispose que : « Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises ».

Conclusion.- Le Règlement européen vient compléter et préciser les obligations déjà prévues par la directive 95/46/CE. En effet, l'étude d'impact visée à l'article 35[972] du Règlement oblige le responsable du traitement à définir de façon précise la finalité du traitement envisagé. Ainsi, grâce à cette étude d'impact, il pèse un véritable obligation d'information renforcée. Si l'introduction de cette analyse d'impact supprime les formalités préalables que devaient accomplir le responsable du traitement, le document d'analyse d'impact permettra au DPD d'agir directement auprès du responsable du traitement. Le DPD apparait comme l'organe principal qui permettra d'assurer le fonctionnement du guichet unique.

Chapitre 2 : Le Délégué à la Protection des Données

Le Règlement européen prévoit la désignation d'un Délégué à la Protection des Données (DPD), traduction française du *Data Protection Officer* (DPO) qui sera obligatoire dans certains cas (section 1) et dont les fonctions sont élargies par rapport à la première version du Règlement (Section 2). La consécration de cet organe régulateur au sein des entreprises et organismes a fait l'objet de nombreuses discussions car il était prévu par le projet de Règlement initial que la désignation d'un DPD serait obligatoire. Cependant, le Règlement européen de 2016 final, prévoit la désignation d'un DPD selon des conditions moins contraignantes, mais qui demeurent le reflet de la volonté du

[972] Règlement Européen C-2016/679, Op. Cit Loci. Section 3 « analyse relative à la protection des données et consultation préalable, Art. 35 « Analyse d'impact relative à la protection des données ».

législateur européen de réguler les moyens de traitement des données à caractère personnel. La réforme vise notamment à aboutir à une régulation par la centralisation des moyens de protection des données à caractère personnel.

Section 1 : La désignation du DPD

Le Délégué à la Protection des Données apparait comme l'organe principal permettant une harmonisation des moyens de protections des données, notamment pour la mise en place du guichet unique (a). De plus, compte tenu de son rôle important le statut du DPD est clairement définit par le nouveau Règlement européen (b).

a) Un organe de centralisation

275. Fondement.- La désignation du DPD apparaît dans le Règlement comme un nouvel organe de garantie de la protection des données à caractère personnel. Le délégué constitue un nouvel organe de régulation et est le reflet de la conformité du traitement. En effet, le considérant n°77 du Règlement indique que le recours au DPD est la « démonstration par le responsable du traitement ou le sous-traitant du respect du présent règlement[973] ». Le DPD est présenté comme le garant de la *qualité* du traitement des données à caractère personnel. Il ressort du texte européen que le DPD est le reflet des diligences effectuées par le responsable du traitement et du sous-traitant. Le recours au DPD apparaît comme gage de bonne conduite de la part du responsable du traitement, et, plus généralement, des entreprises privées ou publiques. En effet, la désignation du DPD assure la mise en place d'un nouvel organe interne de régulation permettant de démontrer que toutes les mesures ont été mise en place afin d'identifier les « risques liés aux traitements ». La création du DPD par le règlement répond à la volonté affichée par le législateur européen de réguler et de sécuriser le traitement des données à caractère personnel dans l'Union européenne. Pour cela, le DPD intervient dans un but d' « évaluation en terme d'origine, de nature, de probabilité, de gravité et d'identification des meilleures pratiques[974] ». Le DPD répond aux « exigences techniques et organisationnelles » d'une mise en œuvre conforme au nouveau cadre européen du

[973] Considérant n°77 du Règlement européen op. cit. loci.
[974] Ibidem

traitement des données à caractère personnel. Les dispositions concernant le DPD sont prévues dans la continuité des dispositions visant les pouvoirs conférés aux autorités de contrôle. Cette *continuité* dans l'organisation formelle du Règlement permet de mettre en lumière le rôle central du DPD.

276. La portée de la désignation, évolution.- Le Règlement européen offre un rôle central au DPD. Il est vrai que le DPD, qui remplace l'actuel CIL, est appelé à jouer un rôle plus important que celui prévu par les anciennes dispositions de la directive de 1995 et de la « LIL » de 1978 où le CIL apparaissait pour la mise en place de mesures de dispenses, dont les Etats membres avaient la faculté. Le DPD est le garant de l'application des obligations qui pèsent sur le responsable du traitement et le sous-traitant[975]. Le principal apport[976] du Règlement est qu'il confère une portée étendue de la désignation du DPD. C'est-à-dire que le DPD s'applique non seulement au responsable du traitement, mais il s'applique également aux organismes privés et publics. Cette application est valable que l'organisme exploite les données pour son compte ou pour celui d'un tiers.

277. A l'origine, la proposition de Règlement de la Commission européenne de 2012 prévoyait que la désignation d'un DPD devait être obligatoire lorsqu'il s'agissait de l'autorité publique ou d'une entreprise de grande taille. En d'autres termes, la proposition de Règlement se fondait sur l'effectif salarial de l'entreprise pour rendre obligatoire la désignation du DPD. La Commission prévoyait également un deuxième critère fondé sur la nature des traitements. Le considérant n°75 de la proposition de Règlement prévoyait la désignation obligatoire du DPD lorsque l'organisme ou l'entreprise prévoyait que « les activités de bases du responsable du traitement ou du sous-traitant consiste[ai]nt en des traitements, qui du fait de leur nature, de leur portée et/ou de leurs finalités, exigait un suivi régulier et systématique des personnes concernées ». La désignation du DPD était conditionnée par la taille de l'entreprise et obligatoire dès lors que l'entreprise atteignait le seuil de 250 personnes, c'est-à-dire une taille correspondant aux petites et moyennes entreprises[977].

---

[975] Cf supra Les nouvelles obligations du responsable du traitement.

[976] L. Marino, « *Le règlement européen sur la protection des données personnelles: une révolution!* », La Semaine Juridique Edition Générale n° 22, 30 Mai 2016, 628.

[977] Recommandation de la Commission, du 3 avril 1996, concernant la définition des Petites et Moyennes Entreprises (Texte présentant de l'intérêt pour l'EEE), Journal officiel n° L 107 du 30/04/1996 p. 0004 – 0009.

278. L'abandon du critère de l'effectif salarial.- La résolution de la Commission du 12 mars 2014 a remplacé le critère de la taille de l'entreprise et a pris en compte le critère de l'amplitude du traitement effectué par le responsable du traitement. Empreint de pragmatisme, le considérant n°75 de la résolution[978] de la Commission européenne affirme que la désignation du DPD devrait être obligatoire « lorsque le traitement est réalisé dans le secteur public ou lorsque, dans le secteur privé, [et] concerne plus de 5000 personnes sur une période de 12 mois ». L'apport de la résolution tient à ce que la désignation du DPD est conditionnée par le nombre de personnes qui sont concernées par le traitement de données à caractère personnel. La Commission précise, cependant, que les données archivées ne sont pas prises en considération pour la détermination du seuil. La prise en compte du nombre de traitements *actifs* reflète le rôle central du DPD qui devra « être consulté préalablement à la conception, à la fourniture, au développement et à la mise en place de tout système de traitement automatisé des données à caractère personnel, afin de garantir le respect des principes de protection de la vie privée dès la conception et par défaut », et le DPD devra effectuer « cette tâche à plein temps [979]». Néanmoins, la Commission retient que le critère de la nature du traitement « nécessitant un suivi régulier et systématique des personnes concernées » demeure un critère d'appréciation pour décider de la nécessité de désigner un DPD.

279. La désignation du DPD sans condition.- La désignation du DPD est visée aux articles 37 et suivants du Règlement européen du 14 avril 2016. Le §1 prévoit que le responsable du traitement ou le sous-traitant désignent un DPD lorsque :

> *« a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;*
> *b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou*

[978] Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[979] Ibidem.

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. »

Le Règlement définitif ne prend pas en compte la condition du seuil du nombre de personnes concernées par le traitement. En effet, la formulation de l'article 37 b) prend en considération le fait que le traitement est effectué « à grande échelle ». Cette absence de définition précise du seuil est néanmoins rattachée à la qualification de traitements qui exigent un suivi régulier et systématique des personnes concernées. Cette absence de limite fait vraisemblablement écho aux dispositions du Règlement[980] qui confèrent un pouvoir de contrôle aux autorités de contrôle qui pourront *juger* si le traitement peut être qualifié de « traitement à grande échelle ». Sans mentionner si le recours au DPD est obligatoire, la formulation de l'article 37 y invite très fortement car toutes les activités de traitement de données y sont incluses, qu'elles soient privées ou publiques[981].

L'abandon du seuil, adopté par la Commission lors de l'adoption de la résolution du 12 mars 2014, et l'emploi du terme « à grande échelle » semblent démontrer que le Parlement a souhaité ne pas amoindrir l'efficacité la législation interne des Etats membres. Ainsi, le Règlement semble adopter la même position que le Conseil de l'Union l'Européenne qui a affirmé sa réticence à imposer aux Etats membres de l'UE un seuil pour recourir à la désignation d'un DPD, préférant laisser ce choix à la discrétion des Etats membres[982].

280. Le DPD obligatoire pour le traitement de données sensibles.- L'article 37 c) renvoie à l'article 9 concernant le traitement des « données particulières » à caractère personnel. En effet, l'article 9 interdit le traitement de telles données sauf dans les conditions prévues au §2 qui prévoit que le traitement est possible s'il « est conforme au droit de l'Union européenne ». « En tout état de cause[983] », et en application de l'article 37,

[980] Article 51 et suivant du Règlement européen 2016, op. cit. loci.
[981] A l'exception des traitements concernant la sécurité de l'Etat ou les autorités judicaires.
[982] Position du Conseil de l'Union Européenne, n°10227/13 §24, du 31 mai 2013 : « la désignation d'un délégué à la protection des données et été rendue facultative, tout en permettant au droit de l'Union ou d'un État membre de rendre cette désignation obligatoire » page 9.
[983] Formulation de l'article 37 op. cit. loci.

le Règlement permet le traitement de telles[984] données lorsque le responsable du traitement et le sous-traitant ont recours à la désignation d'un DPD. Cette disposition implique que les entreprises de fourniture de biens et services en ligne devront recourir à la désignation d'un DPD pour être conformes au nouveau Règlement européen. C'est notamment le cas pour les éditeurs d'applications de santé qui, par définition, entrent dans le critère des traitements qui nécessitent « un suivi systématique des personnes concernées ».

281. Les possibilités de modulations.- L'article 37 §2 du Règlement prévoit que le recours au DPD n'est pas nécessairement unique à chaque entreprise ou organisme, il peut faire l'objet d'une désignation commune. C'est-à-dire qu' « un groupe d'entreprises peut désigner un délégué principal à la protection des données[985] ». Cette disposition est reprise par le Règlement en 2016, alors que le texte de compromis avait opté pour un DPD unique à chaque entreprise ou organisme. Cette modulation est également prévue lorsqu'il s'agit d'un traitement de données effectué par un organisme public. En effet, le §3 de l'article 37 prévoit que « lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type ». Le même paragraphe prévoit cependant que la taille de ces organismes devra être prise en compte dans le cas où ils prévoient de désigner un DPD commun. Cette nuance est en réalité un renvoi à la condition du paragraphe précédent qui prévoit que la mutualisation du DPD n'est possible qu'à partir du moment où il est facilement « joignable à partir de chaque lieu d'établissement ».
Même si le terme « d'obligation » n'est pas inscrit, les nouvelles mesures organisationnelles prévues par le Règlement concourent nettement à la mise en œuvre du guichet unique, en prévoyant l'instauration d'interlocuteurs référents qui ont pour objectif de centraliser la mise œuvre de la protection des données à caractère personnel.

[984] Révélant « l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. » article 9 du Règlement européen op. cit. loci.
[985] Article 35 de la résolution.

b) Le statut du Délégué à la Protection des Données

282. La garantie d'indépendance du DPD.- Alors que la directive de 1995 confiait à chaque Etat membre le soin de définir le statut du CIL et son indépendance fonctionnelle[986], l'article 38 du Règlement vise les garanties d'indépendance et les conditions incombant au statut du DPD durant l'exercice de ses missions au sein d'une entreprise ou d'un organisme. Les conditions visées par l'article 38 §1 font écho à la loi «Informatique et Libertés». En effet, il appartient au responsable du traitement et au sous-traitant de veiller « à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ». Pour cela, le DPD ne doit en aucun cas recevoir d'instructions sur l'exercice de ses fonctions. Il ressort du §2 du même article que le responsable du traitement et le sous-traitant doivent concourir à l'information du DPD en lui permettant « d'entretenir ses connaissances spécialisées ». Cette obligation peut être interprétée comme une obligation de formation continue[987] due par l'employeur à son salarié. C'est ce que prévoyait le considérant n° 75 *bis* de la résolution législative de la Commission qui affirmait que, pour maintenir ses connaissances, le DPD devrait être invité à « participer à des programmes de formation avancée afin de tenir à jour les connaissances spécialisées requises dans le cadre de l'exécution de ses tâches » par le responsable du traitement et le sous-traitant.

Cette *obligation de formation* se justifie d'autant plus que le responsable du traitement et le sous-traitant devront fournir tous les éléments relatifs à la mise œuvre du traitement, lesquels lui permettront de juger s'ils sont conformes à la finalité du traitement.

Cette indépendance fonctionnelle du DPD est consacrée par le Règlement qui prévoit que l'obligation « d'aider » le DPD dans l'exercice de ses fonctions est centrale car le DPD devra faire « directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ».

283. La désignation d'un DPD interne ou externe.- Conformément à l'article 37 §6 du Règlement, le DPD peut être un membre du personnel de l'entreprise ou exercer ses missions « sur la base d'un contrat de service » lorsque le DPD est employé par une entreprise de prestation extérieure. Si le DPD est un employé de l'entreprise ou de

[986] Article 18, 2) alinéa 4 de la directive européenne de 1995 op. cit. loci.
[987] Code du travail : articles L6321-1 à L6321-2

l'organisme, la résolution législative indique qu'il appartient au responsable du traitement ou au sous-traitant de veiller à ce que d'éventuelles autres fonctions professionnelles du délégué à la protection des données soient compatibles avec les tâches et fonctions de cette personne en qualité de délégué à la protection des données et n'entraînent pas de conflit d'intérêts ». C'est également ce que prévoit l'article 38 §6 du Règlement de 2016.

284. Obligation d'information des personnes concernées par le traitement.- Au titre de l'obligation d'information prévue aux articles 13 et 14 du Règlement, les coordonnées du DPD doivent faire l'objet d'une publicité auprès des personnes concernées par le traitement.

Section 2 : Les fonctions du DPD

285. Qualifications.- L'article 37 §5 du Règlement européen prévoit qu'il appartient au responsable du traitement et du sous-traitant de s'assurer que « le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions ». Le Règlement européen ne fait pas référence au niveau de qualification requis pour exercer la fonction de DPD, pourtant, la résolution de la Commission prévoyait l'obligation pour le responsable du traitement de prendre en considération « le niveau du traitement des données » pour effectuer la désignation du DPD.[988]

286. Les missions du DPD.- L'article 39 §1 du règlement prévoit que le DPD a pour missions :

> *a) d'informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;*

[988] Article 35 de la résolution législative de la Commission op. cit. loci.

b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;

c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35;

d) coopérer avec l'autorité de contrôle;

e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.

On remarque que les missions du DPD sont sensiblement les mêmes que celles déléguées au CIL[989] en France. Cependant, le DPD doit, selon le §2 de l'article 39, « être un point de contact » avec l'autorité de contrôle. Il doit également rendre compte de l'état de l'accomplissement de ses missions et des risques qui sont liés au traitement des données.
Cependant, il semble que la Commission ait souhaité une simplification des missions du DPD car la résolution votée en mars 2014 ne prévoyait pas moins de huit obligations supplémentaires à celles du CIL français. En effet, l'article 37 de la résolution prévoyait que le DPD avait l'obligation de conserver une trace écrite de son activité[990], de « contrôler la mise en œuvre et l'application des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris la répartition des responsabilités, la formation du personnel participant aux traitements, et les audits s'y rapportant [991]», de « contrôler la documentation, la notification et la communication relatives aux violations de données à caractère personne[992] », de « vérifier que le responsable du traitement ou le sous-traitant a réalisé l'analyse d'impact relative à la protection des données, et que les demandes d'autorisation ou de consultation préalables

[989] Cf supra page 101.
[990] Résolution article 37 a).
[991] Résolution article 37 b).
[992] Résolution article 37 e).

ont été introduites, si elles sont requises[993] », de « vérifier qu'il a été répondu aux demandes de l'autorité de contrôle et, dans le domaine de compétence du délégué à la protection des données, coopérer avec l'autorité de contrôle, à la demande de celle-ci ou à l'initiative du délégué à la protection des données [994]», « veiller au respect du présent règlement dans le cadre du mécanisme de consultation préalable [995]» et, enfin, d'« informer les représentants des travailleurs au sujet du traitement des données des travailleurs [996]».

Conclusion.- Si ces obligations ne sont pas expressément énumérées dans les missions du DPD, elles sont toutefois prévues par les nouvelles obligations du responsable du traitement et du sous-traitant qui doivent effectuer et transmettre aux autorités de contrôle la documentation relative à l'étude d'impact du traitement des données et la documentation relative aux nouvelles obligations de sécurité[997].

[993] Résolution article 37 f).
[994] Résolution article 37 g).
[995] Résolution article 37 i).
[996] Résolution article 37 j).
[997] Cf supra les nouvelles obligations du responsable du traitement.

Conclusion générale

Cela fait 38 ans que la loi «Informatique et Libertés» originelle[998] a été promulguée. Elle a fait l'objet d'une modification par la loi du 6 août 2004[999] issue de la directive européenne n°95/46/CE du 27 octobre 1995. Cela fait plus de 10 ans que les dispositions relatives au traitement des données à caractère personnel permettent de dresser une protection des droits et libertés des personnes. Cependant, au vu des différents développements de cette étude, les nouvelles capacités de traitement n'ont-elles pas conduit à se demander si une refonte des textes relatifs à la protection des données n'était pas souhaitable ? Certains commentateurs, lors de la réforme de 2004, indiquaient, non sans ironie, que les dispositions relatives à la protection des données à caractère personnel ressemblaient à l'Arlésienne[1000] . Néanmoins, si la « multiplication des textes […] a un effet déplorable quant à l'utilisation du texte[1001] », il n'en demeure pas moins que la reconfiguration de la protection des données à caractère personnel est marquée par la continuité de son champ d'application. En effet, la réforme par la loi du 6 août 2004 précise les traitements encadrés par la protection des données, permettant ainsi une application large de la notion de « donnée à caractère personnel ».

287. Le renforcement des principes préexistants.- Il est incontestable que l'adoption de la loi «Informatique et Libertés», en 1978, constituait une innovation en termes de protection, mais le texte est apparu comme « rapidement inadapté » avec la multiplication des échanges internationaux[1002]. Comme envisagé dans cette étude, la directive de 1995 avait pour objectif principal d'éviter la dispersion des textes relatifs à la protection des données personnelles. C'est avec le même objectif que la Commission et le Parlement européen ont décidé de poursuivre l'harmonisation des moyens de traitement, en adoptant le 27 avril 2016 le Règlement européen relatif à la protection et à la circulation des données à caractère personnel. Outre la nature contraignante du texte, le Règlement européen apporte de nombreuses définitions en matière de traitement. En effet, l'article 4 du Règlement consacre pas moins de 26 alinéas qui définissent ce que recouvrent la notion

[998] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, version initiale, JORF du 7 janvier 1978, p 227.
[999] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1000] J. Frayssinet, « *La loi relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture* », Lamy droit de l'immatériel 2005, n°9, dossier spécial.
[1001] Ibidem note précédente.
[1002] M. Vivant, « *Comment gérer un traitement de données personnelles ?* », Le Lamy droit du numérique 2016, Guide pratique, n°4233.

de traitement et la notion de donnée à caractère personnel[1003]. Cependant, la loi «Informatique et Libertés» modifiée par la loi du 6 août 2004 permettait de renforcer les prérogatives des personnes concernées par le traitement de ses données personnelles. En effet, le droit d'opposition et le droit à l'information faisaient l'objet d'un renforcement, notamment en imposant au responsable du traitement de prouver qu'il avait mis tout en œuvre pour permettre à la personne concernée d'exercer son droit.

C'est avec des intentions plus « ambitieuses[1004] » que le Règlement européen a été adopté. En effet, le texte consacre le droit au déréférencement, nommé à l'origine « droit à l'oubli », dégagé par le célèbre arrêt *Google Spain*[1005] du 13 mai 2014. La décision de la CJUE a été qualifiée de « révolutionnaire[1006] » par certains auteurs qui y ont vu la consécration d'une véritable maîtrise des données personnelles permettant l'avènement d'un « Habeas Corpus[1007] » numérique. Le Règlement européen vise notamment à concilier le respect de la vie privée et la libre circulation des données au sein de l'Union européenne. Comme envisagé dans cette étude, la conciliation de ces deux principes ne peut être effective que par la combinaison du droit à l'information et du droit d'accès conférant une véritable valeur au *consentement* de la personne. La reconnaissance de ces droits permettrait de rééquilibrer les rapports entre le responsable du traitement et la personne concernée, dont la portée n'est que « balbutiante[1008] » dans la loi «Informatique et Libertés» modifiée par la loi du 6 août 2004. Le renforcement des droits préexistants par le règlement est justifié par le fait qu'il est admis, aujourd'hui, que les informations collectées sur internet sont rattachées à la personne et permettent de l'identifier. De plus, le développement des nouveaux moyens de traitement sous-tendent l'apparition d'une identité « numérique » qui est rattachée à la personne[1009]. C'est parce que les données sont

[1003] L'article 2 de la directive de 1995 consacrait déjà 9 alinéas à la définition des notions de traitements et de données à caractère personnel.
[1004] M. Vivant, « *Comment gérer un traitement de données personnelles ?* », Le Lamy droit du numérique 2016, Guide pratique, n°4233.
[1005] Arrêt de la Cour (grande chambre) du 13 mai 2014, Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, affaire C-11/12.
[1006] L. Marino, « Le règlement européen sur la protection des données personnelles : une révolution ! », La Semaine Juridique Edition Générale n°22, 30 mai 2016, n°628.
[1007] Projet de loi « République Numérique » défendu par Axelle Lemaire et présenté à l'Assemblée Nationale le 15 décembre 2015.
[1008] J. Frayssinet, « *La loi relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture* », Lamy droit de l'immatériel 2005, n°9, dossier spécial.
[1009] Conseil d'Etat, rapport « Le numérique et les droits fondamentaux », 2014.

rattachées à l'identité de la personne que le droit de les maîtriser directement peut être qualifié de droit de la personnalité.

288. Le renforcement du droit à l'information et une plus grande place au consentement apparaissent aussi avec l'apport de définitions claires pour certaines données sensibles comme les données de santé ou « relatives à l'état de santé [1010]». Ces données nécessitent un « acte positif clair » qui doit permettre de déterminer la valeur du consentement. Ce dernier devenant une volonté autonome et différente du droit d'opposition. Le renforcement des obligations du responsable du traitement concernant le recueil d'un consentement libre et clair apparaît comme une nécessité compte tenu de la multiplicité des sources contenant des données à caractère personnel. Les exemples de cette étude démontrent qu'un grand nombre de données issues de « nos » vies est collecté. Ces données sont ensuite traitées pour être enfin valorisées dans un contexte[1011]. C'est pourquoi, il est apparut nécessaire pour les citoyens de maîtriser l'usage qui est fait de leurs données personnelles. Cela a conduit certains acteurs à envisager un « droit de propriété » sur ces données. Cependant, cela conduirait, par voie de conséquence, à envisager la cessibilité de ces données, en particulier pour des raisons économiques. Cette perspective a été considérée par le Conseil d'État comme un risque pour les citoyens. En effet, la multiplication des opportunités offertes par les acteurs économiques, en particulier commerciaux, dans le domaine de la santé, de valoriser ces données pourrait mener à des situations présentant de nouveaux risques pour les libertés individuelles. La publication des données relatives à la forme et à la santé (par exemple, sur les réseaux sociaux) peut aussi devenir un outil de contrôle économique et social voire de « profilage » des risques associés à un individu. Les craintes concernant l'utilisation des données personnelles sont d'autant plus légitimes que des données personnelles, en apparence anodines, peuvent être intégrées dans des algorithmes d'évaluation des risques pour la santé. Ainsi, l'achat d'une friteuse ou la consommation de substances riches en graisses pourraient participer à l'élévation des risques de pathologies cardio-vasculaires d'un usager. Lorsque les dispositifs de captation d'informations de santé seront intégrés dans l'ensemble des terminaux mobiles et objets connectés (comme les nouvelles générations de montres

[1010] Article 4 alinéa 15 du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[1011] Cf supra Introduction, et chapitre 3 « la spécificité de la protection des données de santé ».

connectées) ou les vêtements et accessoires sportifs, le recueil de ces informations pourrait devenir encore plus sensible en termes d'évaluation précise du profil des risques associés à une personne. Ainsi, la transmission non-contrôlée de ces informations à des annonceurs pourrait avoir des conséquences imprévisibles. Or, la cession ou la location des données personnelles ne peuvent être accueillies de façon favorable, ceci en raison de l'attachement de ses informations à la personne. En vertu de l'article 16-4 du Code civil, il paraît donc indispensable que l'obtention du consentement soit plus encadrée, tant par un cadre légal que par la mise en place d'un processus formel. Ce dernier permettant à la personne concernée par le traitement de délivrer un consentement libre et éclairé. Cette exigence de redéfinir l'expression « numérique » du consentement[1012] doit permettre de faire peser sur le responsable du traitement la responsabilité d'apporter la preuve que la personne concernée a consenti à ce que ses informations soient stockées et traitées. En plus de la preuve d'un consentement éclairé, en vertu du caractère immuable et incessible du consentement au traitement des données personnelles, le responsable doit apporter la preuve que le consentement n'a pas été « réputé acquis » au cours des différents traitements. Au fil du temps, des doutes peuvent survenir quant à la question de savoir si le consentement initialement fondé sur des informations valides reste valable. « Les gens changent souvent d'avis pour diverses raisons, parce que leur choix initial a été opéré sans y prendre garde ou parce que les circonstances ont changé[1013]. ». C'est la raison pour laquelle, à titre de bonne pratique, les responsables du traitement devraient s'efforcer de réexaminer, au bout d'un certain temps, le choix d'une personne en l'informant, par exemple, de son choix actuel et en lui offrant la possibilité de le confirmer ou de l'infirmer[1014]. Ces garanties permettraient à la personne concernée par le traitement de disposer de tous les éléments lui permettant, si besoin, de prouver son intérêt à agir en justice.

289. La mise en place d'outils juridiquement reconnus permettant l'expression d'un consentement clair ainsi que sa réitération[1015], combinés à une obligation d'information renforcée pesant sur les prestataires techniques, au même titre que l'obligation qui pèse sur

[1012] Article 7 de la proposition de règlement du Parlement de la commission relatif à la protection des données personnelles sec. 2012 72 et 73.
[1013] Comme le précise le groupe de travail « article 29 » dans son avis 15/2011 sur la définition du consentement adopté le 13 juillet 2011.
[1014] Ibidem.
[1015] Même si aucune condition d'adhésion ne varie dans le temps.

les professionnels de santé[1016] ou l'administration publique, est une solution qui devrait être mise en place. Cette obligation *renforcée* d'information est prévue par le texte européen avec l'obligation pour le responsable du traitement de rédiger une « étude d'impact sur la personne » dont les données sont traitées.

290. Les modalités d'exercice des droits modifiées.- Le développement des Nouvelles Technologies de l'Information et de Communication (NTIC) renvoie à un mouvement qui prône « l'ouverture des données », généralement nommé « Big Data ». S'il est certain que le traitement massif de données présente un risque d'atteinte aux droits et libertés des personnes, il faut également en reconnaître les avantages. Les craintes du « Big Data » proviennent, historiquement, de la peur d'un fichage général de la population lors de la mise en place du projet SAFARI. La notion de « Big Data » est associée à une règle nommée « 3V » c'est-à-dire Volume, Vélocité et Variété. Il est affirmé par certains auteurs[1017] que l'objectif du Big Data n'est pas « *l'information ».* C'est-à-dire que l'intérêt du Big Data ne réside pas dans *l'interprétation* de l'information mais dans la manipulation des données brutes. Cependant, toutes les données accumulées, rassemblées et transformées en masses sont « utiles pour la maîtrise de machines, de notre vie sociale » et laissent des traces[1018]. Les capacités *positives* du « Big Data » sont réelles dans le sens où elles permettent, en matière de santé[1019], de connaître la progression d'une épidémie ou de détecter des interactions médicamenteuses à risques[1020]. Par exemple, la société IBM a mis en place un logiciel et des algorithmes ayant un raisonnement (mathématique) proche de celui de l'homme. Il est utilisé dans le domaine médical pour effectuer des diagnostics. Il intègre des données telles que les remarques du praticien, les entrevues avec le patient, les résultats d'analyses, mais, également, des données comme les antécédents familiaux. L'intégration d'algorithmes « cognitifs » est la preuve que les technologies sont de plus en plus maîtrisées par les concepteurs[1021]. Leur utilisation doit faire l'objet d'un encadrement légal renforcé, notamment dans le domaine de la santé.

[1016] Article 1110-4 CSP.
[1017] J-C Cointot, Y. Eychenne, « La révolution Big Data, les données au cœur de la transformation de l'entreprise », Ed. Dunod, 2014.
[1018] P. Delort, « Le Big Data », Ed. Puf, coll. « Que sais-je », 2015.
[1019] Dr. J. Lucas, « Les enjeux du « Big Data » dans le domaine de la santé », Ethique & Société, Vol. 16 n°61, mars 2016.
[1020] G. Babinet, « Big Data, penser l'Homme et le monde autrement, vivre mieux et en meilleure santé », Ed. Le Passeur, p 65.
[1021] IBM, « *Watson travaillera en français en 2016 »*, *Le Monde informatique,* 22 septembre 2015.

291. La place du secret face à l'Information.- Le secret professionnel et la confidentialité sont les garanties principales qui permettent de contrôler l'échange des informations médicales entre le patient et les professionnels. Cependant, les indiscrétions sont toujours possibles ; la négligence ou le manque d'information concernant l'importance et les enjeux qui entourent les informations sont présents à chaque étape de la transmission des données de santé[1022].

La nécessité d'une gestion rigoureuse des droits d'accès est un préalable fondamental à la mise en place des dossiers médicaux informatisés ou de prestations de santé connectée. Conformément à l'article L.1110-4 du Code de la santé publique, nul ne doit avoir accès au moindre élément du dossier d'un patient s'il ne participe pas aux soins de ce patient. La difficulté de ce droit d'accès tient également à la formulation des textes qui limite le partage et l'intervention aux « professionnels de santé » ou aux personnes « qui participent aux soins ». Or, les risques de fuite des informations sont d'autant plus grands avec l'externalisation des données de santé par le système d'hébergement dont les gestionnaires ou les propriétaires ne sont pas nécessairement titulaires d'un titre leur permettant d'exercer en tant que « professionnel de santé » ou de participer aux soins. Pour certains, la loi de modernisation de notre système de santé votée le 26 janvier 2016[1023] aurait pour conséquence « la disparition du secret médical », car elle permettrait l'ouverture du partage des données de santé. Cette ouverture se traduirait notamment par « l'accessibilité de ces données nominatives via un simple site internet ou à des entités privées et publiques qui seraient labélisées par le ministère »[1024].

292. Or, comme envisagé dans cette étude, il convient d'élargir la compétence des autorités de contrôle aux différents prestataires privés ou publics, en particulier vis-à-vis des entreprises qui proposent des prestations de santé via les Nouvelles Technologies d'Information et de Communication (NTIC), afin de garantir le respect des libertés fondamentales. L'élargissement de ces compétences doit s'envisager au vu de nos principes et lois déjà édictés, notamment avec l'analyse des principes généraux de confidentialité et de sécurité. L'élargissement des compétences des AAI comme la HAS ou d'association comme le COFRAC permettrait de contrôler les professionnels des technologies de l'informatique, tels que les hébergeurs de données et les éditeurs, qui ne

[1022] Position du Conseil Consultatif National d'Ethique avis n°104 du 29 mai 2008.
[1023] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.
[1024] F. Bizard, « La vraie bombe de la réforme Touraine : La disparition du secret médical », Atlantico, 18 mars 2015.

sont pas soumis au cadre réglementaire médical. Cette analyse doit également s'effectuer en fonction des normes européennes, notamment vis-à-vis du règlement du 27 avril 2016 sur la circulation des données personnelles[1025], afin de créer un système d'exploitation accessible au grand public dans le respect des libertés fondamentales. Actuellement, la protection des données de santé est une préoccupation capitale, dans un contexte où l'administration de l'assurance maladie et le législateur souhaitent unifier la gestion des informations de santé à travers le déploiement des TIC et du DMP. Les informations médicales à caractère personnel relèvent de la « sphère privée », pour reprendre les propos de Monsieur le Professeur Carbonnier. Cette sphère est cependant propice à l'intrusion, notamment avec le développement des NTIC. Dans le cadre de l'hébergement des données médicales, l'agrément auquel sont soumis les contrats - et non les dispositifs de traitement - est perfectible. En effet, le patient ne sait pas que ses données sont hébergées et qu'il peut lui-même y accéder directement. Cette situation s'explique par le fait qu'il est souvent déduit, à tort, un consentement du patient à ce que les données et les informations le concernant soient partagées. Si ce consentement implicite est toléré dans le cadre du secret partagé au sein d'un service hospitalier, le consentement semble être passif, dans le cadre de la médecine libérale, par la remise de la carte vitale. L'information soumise à un double consentement du patient pourrait être une alternative intéressante. Le patient exprimerait son consentement, non seulement aux soins, mais, également, à ce que les informations qui en émanent soient informatisées, partagées et hébergées. Dans la majeure partie des cas, il ne sait pas que ses informations sont amenées à transiter par un responsable du traitement dont il ne connaît ni l'identité ni la finalité de la mission. Le règlement européen donne un axe de réflexion en prévoyant que le document relatif au consentement devra être distinct de tout autre document. Dans le cadre de la médecine en cabinet libéral, il serait envisageable que la remise de la Carte Vitale ne soit pas considérée comme l'expression d'un consentement implicite. Une méthode d'authentification pourrait permettre de conclure à l'accord du patient, comme prévu par le système SSL, sur le modèle de la carte bancaire. Cette méthode permettrait de faire peser sur le médecin une obligation d'information renforcée vis-à-vis du patient. Il devrait l'informer de la finalité du traitement de ses informations et lui indiquer son droit de s'opposer ou de masquer certaines informations lors de l'accès à son dossier. L'information serait alors précise, loyale et complète, comme visée dans le Code de la santé publique et conforme au «

[1025] Règlement européen (UE) du 27 avril 2016 op. cit. loci.

principe de finalité des traitements » de la directive européenne 95/46/CE relative aux traitements des données à caractère personnel. Cette méthode va dans le sens du Règlement européen du 27 avril 2016. De plus, le texte européen prévoit que le traitement des données sensibles telles que les données de santé nécessite la désignation d'un Délégué à la Protection des Données (DPD). Ce dernier a pour mission, non seulement de s'assurer de la licéité du traitement, mais, aussi, d'assurer que les droits des personnes sont garantis.

293. Une régulation des données de santé (à caractère personnel) ?- Une réforme des obligations des prestataires techniques et des éditeurs de logiciels, concernant la rédaction des contrats d'adhésion permettrait de renforcer la transparence des conditions d'accès aux services numériques. En effet, une interface accessible et claire, mettant en évidence les phases clefs, comme le recueil du consentement[1026] et la collecte des données sensibles, notamment via l'utilisation d'icones ou de codes visuels normalisés, permettrait à la personne concernée par le traitement d'avoir un comportement « actif » lors du dépôt de ses informations. Il convient de solliciter le consentement de la personne qui dépose ses données de santé, notamment par le système instauré par la nouvelle norme simplifiée de la CNIL de la « case à cocher ». En outre, freiner la rapidité de la transaction ne saurait suffire à l'expression d'un consentement libre et éclairé. La réitération du consentement de la personne concernée par le traitement est primordiale dans le domaine de la santé en raison de la sensibilité des données. L'un des champs les plus complexes et les plus prometteurs, mais aussi des plus inquiétants, concerne la santé et la prévention. Ce mouvement qui repose sur une utilisation croissante de capteurs corporels connectés – bracelets, podomètres, balances, tensiomètres, etc. – et d'applications sur mobiles, s'accompagnent de pratiques volontaires d'auto-quantification. Ce mouvement se traduit par l'utilisation de modes de captures de données de plus en plus automatisés et par le partage et la circulation de volumes considérables de données personnelles. Il s'agit d'un phénomène qui se développe à l'initiative des individus eux-mêmes, mais aussi, en raison des modèles économiques des acteurs investissant ce marché.

294. L'objectif de la production de masse de leurs données numériques et l'analyse en vue de leur valorisation sont devenus un enjeu de compétitivité pour les entreprises. Plus que les caractéristiques du Big Data, ce sont les possibilités d'analyse des

[1026] Notamment par le biais de couleurs comme le suggère le professeur V. Gautrais « La couleur du consentement électronique » cahiers de la propriété intellectuelle page 78.

informations, qui deviennent, dès à présent, l'enjeu stratégique de l'économie de la donnée. Monsieur Brasseur[1027] explique qu'en matière de marketing, « nous sommes en train de passer d'un modèle classique de segmentation à un modèle de caractérisation comportementale. […] Le « profiling » des clients apporte, sans aucun doute une valeur ajoutée à l'entreprise qui peut alors analyser et personnaliser ses produits et ses offres. » Ainsi, dans la publicité, le Big Data permet de mettre de nouveaux outils à la disposition des PME et TPE, en leur donnant la possibilité de développer leur activité d'une manière inédite.

295. Ainsi, les données « nous » concernant présentent, de façon certaine, une valeur économique qui ne cesse de croître. Les données personnelles qui « retracent notre vie » sont collectées via nos smartphones et différents objets. Ces données, souvent produites volontairement par la personne, présentent un intérêt certain pour le corps médical. Néanmoins, aucune régulation juridique spécifique permettant de *basculer* du « caractère personnel » au « caractère médical classique » n'est prévue. Or, les données issues des NTIC, comme celles du « quantified self » ne se prêtent pas « à un appréhension juridique binaire oscillant entre la surprotection des données sensibles et l'absence de toute protection »[1028]. Il semble donc, qu'un régime prenant en compte le contexte inédit « du » traitement des données de santé soit sur le point d'apparaître. De plus, le nouveau règlement européen sera très certainement le vecteur d'une régulation juridique innovante en termes de protection des personnes. Cette régulation permettra de garantir l'équilibre entre l'innovation technologique et l'intérêt des personnes. Comme le prévoit le règlement, les Etats membres devront notifier à la Commission les dispositions légales qu'ils adoptent, en vertu du Règlement européen, au plus tard le 25 mai 2018.

[1027] C. Brasseur, « Enjeux et usages du Big Data, technologies, méthodes et mise en œuvre », Lavoisier, Hermès Science, 2013.
[1028] A. Mendoza-Caminade, « Big Data et données de santé : quelles régulations juridique ? », Revue Lamy Droit de l'Immatériel, 2016, n°127.

Bibliographie

Ouvrages :

AFDS. Consentement et Santé, Collection Thèmes et Commentaires, Dalloz, 2014.

BABINET, G. Big Data, penser l'Homme et le monde autrement, 2015, Edition Le Passeur.

BALLE, F. Lexique d'information-communication, collection lexique, Dalloz 2006.

BEIGNIER, B. Le droit de la personnalité, Edition Puf. Collection « Que sais-je ? », 1992.

BERGOIGNAN-ESPER, C. / SARGOS, P. Les grands arrêts de droit de la santé, Collection arrêts, Dalloz, 2010.

BOULOC, B. Droit pénal général, Collection Précis, Dalloz, 2013.

BRASSEUR, C. Enjeux et usages du Big Data, technologies, méthodes et mise en oeuvre, Lavoisier, Hermès Science, 2013

CARDON, D. « *A quoi rêvent les algorithmes, Nos Vies à L'heure des Big Data* », Edition Seuil, La République des Idées, Octobre 2015.

CASTET-RENARD, C. « Droit de l'internet ; Droit français et européen », Montchrestien, Edition Lextenso, 2012.

COINTOT J-C, EYCHENNE, Y. « *La révolution Big Data, les données au cœur de la transformation de l'entreprise* », Edition Dunod, 2014.

DEBET, A. / MASSOT, J. / METALLINOS, N. « La protection des données à caractère personnel en droit français et européen », Informatique et Libertés Collection. Les intégrales 2015, n°10, Edition Lextenso.

DELORT, **P.** « *Le Big Data* », Edition Puf, Collection « Que sais-je », 2015.

DESGENS-PASANAU, G. « La protection des données personnelles », 2ème édition, Lextenso, 2012.

FRANCQ, S./ O. DE SCHUTTER, « la proposition de directive relative aux services dans le marché intérieur : reconnaissance mutuelle, harmonisation et conflits de la loi dans l'Europe en ligne, Cahiers de droit européen*,* 2005, p.604 et s.

GALINON-MEMENEC, B. / ZLITNI, S. / LIENARD, F. « *L'Homme-trace, Inscriptions corporelles et techniques* », Collection CNRS Alpha, 30 décembre 2015.

GILLIAN, J. Introduction au droit et éléments de droit civil- Larcier 2000.

LARGUIEZ J. / CONTE P. /FOURNIE S. Droit pénal spécial, Collection Mémentos, Dalloz, 2013.

LAUDE, A. / MATHIEU, B. / TABUTEAU, D. Droit de la santé, Edition Puf, Collection Thémis droit, 2012.

LUCAS, A. / DEVEZE, J. / FRAYSSINET, J. « *Droit de l'informatique et de l'internet »,* Edition PUF, Collection Thèmis droit privé, 2001, n°113.

RENUCCI, F. « *Introduction générale à la Convention européenne des Droits de l'Homme Droits garantis et mécanisme de protection* », Edition Conseil de l'Europe, 2005.

TANQUEREL, J.J. Le serment d'hypocrite, Edition Max Milo 2014.

TERRE, F. / FENOUILLET, D. Droit Civil, Collection Précis, Dalloz, 2013.

TERRE, F. / FENOUILLET, D. « Droit civil. Les personnes, » Dalloz Collection Précis, 8ième édition, octobre 2012.

ZORN-MACREZ, C. Données de santé et secret partagé, Collection « santé, qualité de vie et handicap », Presses Universitaires de Nancy 2010.

Thèses et Mémoires :

BERTRAND, M. Le dossier Pharmaceutique au service du pharmacien : Un outil informatique construit pour une utilisation professionnelle optimale, thèse en Pharmacie, 2012.

CHEVILLARD, M. Le droit au masquage par le patient dans le cadre du dossier médical personnel en France, thèse en médecine générale, Université Paris VI Pierre et Marie Curie, 2007.

COULIBALY, I. La protection des données à caractère personnel dans le domaine de la recherche. Thèse de droit privée, Université de Grenoble, 2011.

DELCAMBRE, R. Les algorithmes de fouille de données, CNAM, 2005.

DUASO, CALES, R. Principe de finalité, protection des renseignements personnels et secteur public : Etude sur la gouvernance des structures en réseau, thèse de droit, 2011.

LACOSTE, J-M. Pour une pleine et entière reconnaissance du droit à la protection des données à caractère personnel, Université Toulouse Capitole I, 2008.

LE CLAINCHE, J. La protection des données personnelles nominatives dans le cadre de la recherche dans le domaine de la santé Université Montpellier I Faculté de droit, des Sciences Economiques et de Gestion, 2008.

WILPART, M. Secret médical et assurances de personnes, thèse de droit privé, Université Jean Moulin Lyon 3, 2009.

Articles et revues Juridiques :

ACTUALITE DU DROIT EUROPEEN, « *La protection des données à caractère personnel* », Droit Fondamentaux, L'observateur de Bruxelles, n°105, juillet 2016, Edition. Larcier, Page 81.

ALT-MAES, F. « *La liberté de conscience accordée aux personnes tenues au secret professionnel* », RSC 1998. Page 301.

AUTIN, J-L. « *Le devenir des Autorités Administratives Indépendantes* »**,** RFDA 2010, page 875

BACACHE-GIBEILI, M. « *Le secret médical partagé »,* Gaz. Pal. 30 décembre 2008 n° 365, page 44.

BADINTER, R. *« le droit au respect de la vie privée* », JCP 1968, I n°2136.

BENSOUSSAN, A. « *Le droit à l'oubli sur Internet* », Gaz. Pal., 6 févr. 2010, no 37, p. 3.

BENSOUSSAN, A. *« Le correspondant à la protection des données à caractère personnel : un maillon important de la réforme* », Gaz. Pal. n°286 12 octobre 2004

BERGUIG, M. et THIERACHE, C. « *L'oubli numérique est-il de droit face à une mémoire numérique illimitée ?* », RLDI 2010/62, no 2039.

BOSKOVIC, O. *« Télémédecine : aspects de droit international privé »,* RDSS 2011, page 1021**.**

BOSSI, J. « *Comment organiser aujourd'hui en France la protection des données de santé »,* RDSS 2010, page 208.

BOURDAIRE-MIGNOT, C. *« Téléconsultation : quelles exigences ? Quelles pratiques »,* RDSS 2011, page 1003.

CARON, CH. « *A propos du conflit entre les œuvre de fiction et la vie privée* », D. 2003, jur, P. 1715.

CEDILE, G. « *Le signalement par le psychologue est-il compatible avec le respect du secret professionnel ? »,* AJ pénal 2011, page 579.

CHOCQUE, J-C. / **FU-BOURGNE, X**. *« Impacts et enjeux de l'informatisation dans le système de santé »,* Gazette du Palais, 19 octobre 2000 n° 293, page 15.

CNIL, La « signature vocale », Voix, Image et protection des données personnelles, La Doc. Fr., 1996.

CRESSARD, P. « *L'actualité de notre secret médical* », Bulletin de l'ordre des médecins, Février 2006, n°2, édito.

DAOUD, E. *« Libertés fondamentales et protection des données personnelles »,* Rev. Lamy Droit des Affaires, 2013, n°87, Doss. Spéc.

DE GROVE-VALDEYRON, N. *« La directive sur les droits des patients en matière de soins de santé transfrontaliers. Véritable statut juridique européen du patient ou simple clarification d'un régime de mobilité ? »,* RTD Eur. 2011, page 299.

DEBET, A. « *Le champ d'application matériel de la notion de traitement des données à caractère personnel, »* La protection des données à caractère personnel en droit Français et Européen, Edition, Lextenso, 2015.

DELVOIE, A. « *Le correspondant CNIL : une adaptation du « chief privacy officer' américain ?* ». Gaz. Pal. n° 109, 19 avril 2005

DERIEUX, E. « *Protection des données à caractère personnel et activités de communication publique Apports du règlement européen du 27 avril 2016 au regard de la précédente directive du 24 octobre 1995 et de la loi française du 6 janvier 1978 (révisée par celle du 6 août 2004)* », RDLI ,2016 n°128

DEVEZE, J. « *Le vol de « biens informatiques » »,* La Semaine Juridique Edition Générale n°44, 30 octobre 1985. I 3210.

DUPONT-LASSALLE, J. « *Protection des données personnelles* », Europe n°10, Octobre 2014, comm. 368.

EVIN, C. *« Le secret médical dans le cadre hospitalier »*, Recueil Dalloz 2009 page 2639.

FAURE, B. « *Les objectifs de valeur constitutionnelle* », Rev. Fr. Dr. Const. 1995, p. 47 et s.

FAURE, G. / DAURY-FAUVEAU, M / HENOT, F. et autres. « *Chronique de Droit médical numéro 1 »*, 29 mars 2003.

FERRAUD-CIANDET, N. *« Questions juridiques sur l'e-santé »,* Petites affiches, Lextenso 3 mai 2007 n° 89, page 11.

FERRAUD-CIANDET, N. Professeur en droit ; Professeur assistant à Grenoble Ecole de management, L'Union européenne et la télésanté, RTD Eur. 2010 p. 537.

FIESCHI, M. *« Les données du patient partagées : un atout à ne pas gâcher pour faire évoluer le système de santé »,* Droit social 2005 page 80.

FRAYSSINET, J. « *La loi relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture* », Lamy droit de l'immatériel 2005, n°9, dossier spécial.

FRAYSSINET, J. « *le transfert et la protection des données personnelles en provenance de l'Union européenne vers les Etats-Unis : l'accord dit « sphère de sécurité ou Safe Harbor* », JCP, Comm. Com. Electr., mars 2001, page 10.

FRISON-ROCHE, M-A. « *Remarques sur la distinction de la volonté et du consentement en droit des contrats, fiscal et social* » - RTD Civ. 1995 p. 573

GALLOUX, J.C. / GAUMONT-PRAT, H. « *Droits et libertés corporels* » janvier 2006 décembre 2006, Panorama, D. 2007 p 1102, partie c - l'image du corps, 1§ voir aussi 3§ et suivants.

GALLOUX, J.C et GAUMONT-PRAT, H. Droits et libertés corporels : « Panorama de la législation, de la jurisprudence et des avis des instances éthiques », D. 2005, p 536

GAMBARDELLA, S. « *Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé* », RDSS 2016 p.271.

GAUDRAT, P. « *Du logiciel-support à l'illicéité de la propriété privée numérique* » RDT- Com.2002. Page 55.

GAUTIER, P-Y. / LINANT DE BELLEFONDS, X. « *De l'écrit électronique et des signatures qui s'y attachent* », J.C.P.G., n°24, 14 juin 2000, p.1116

GAUTRAIS, V. « la couleur du consentement électronique » cahiers de la propriété intellectuelle, vol.16, no. 1, 2003.

GIRARDOT, Th.-X. « Régime de la déclaration préalable des traitements informatisés d'informations nominatives. » AJDA 1997 p 156,

GOBERT, M. « réflexion sur les sources du droit et les 'principes' d'indisponibilité du corps humain et de l'état des personnes », RTD. Civ. 1992, p 489

HARICHAUX, M. « Les sites portails santé sur Internet : quelles perspectives ? », RDSS 2000. p.697

HARICHAUX, M. Internet pour le droit, Montchrestien, n° 175

HERVEG, H. « *Panorama des responsabilités liées aux services et produits de santé en ligne en droit européen* », RDTI, 2008, n°68 et s.

HOUSSIN, D. « *Le secret médical dans les nouvelles pratiques et les nouveaux champs de la médecine* », Recueil Dalloz 2009, p 2619.

JOB, J.-M. « *la loi Informatique et Libertés » et les données de santé* », RLDI 2008/34 n°1161

PERRAY, R. « *Données à caractère personnel. Formalités préalables à la mise en œuvre d'un traitement de données caractère personnel* », §100 et suivant. Jur.Cl. Administratif, Fasc. 274-30 : Informatique.

KAHN, A. « *Le secret médical : d'Hippocrate à internet »,* Recueil Dalloz 2009, page 2623.

KOUKOUTSAKI-MONNIER, A. « Emmanuel HOOG, Mémoire Année Zéro », Questions de communication [En ligne], 17, 2010, mis en ligne le 23 janvier 2012, consulté le 27 juillet 2016

Lamy, « *Vers la mise en place d'un droit à l'oubli numérique,* » le Lamy Droit des Medias et de la Communication, n°477-50.

LAVERDET, C. « *Données personnelles : bilan de 1995 et réforme de 2014 ? »,* Revue Lamy Droit de l'Immatériel, 2014, page 104.

LE GOFFIC, C. « *Consentement et confidentialité à l'épreuve de la télémédecine »,* RDSS 2011 page 987.

LEPAGE, A. « *Le délateur dénoncé... et condamné* », Rev. Com. com. élec. n°10 oct. 2007, com. n° 126,

LEPAGE, A. *« La notion de vie privée au sens de l'article 8 de a convention Européenne des droit de l'homme ne cesse de prendre de l'ampleur »* D2001.1988 Recueil Dalloz, 2001 page 1988.

LEPAGE, A. « *Les Droits de la personnalité à l'épreuve des grandes affaires criminelles »,* D. 2004, p. 1634.

LEPAGE, A. Personnalité (Droits de la), actualisation juin 2016, septembre 2009, Répertoire de droit civil, section 1.

LUCAS, J. « *Les enjeux du Big Data dans le domaine de la santé »,* Ethique et société, Vol. 16, n°16, Mars 2016**.**

MALLET-PUJOL, N. « *Collecte, utilisation et diffusion des données nominatives à des fins d'enseignement et de recherche ».* http://www.msh-paris.fr, 2002. <edutice-00000033>.

MALLET-PUJOL, N. « *Droit à l'oubli numérique et désindexation : la solution en trompe-l'œil d CJUE »*, Chroniques et opinion, Droits de la personnalité, Légipresse 1er septembre 2014, n°319.

MARINO, L. « *Le règlement européen sur la protection des données personnelles: une révolution!* », La Semaine Juridique Edition Générale n° 22, 30 Mai 2016, 628.

MENDOZA-CAMINADE, A., *« Big Data et données de santé : quelles régulations juridique ?* », Revue Lamy Droit de l'Immatériel, 2016, n°127.

MESTRE, J. / **FAGES, B.** « *Le secret professionnel »*, RDT, civ 2005, page 384.

MÉTALLINOS, N. / BOTCHORICHVILI, N. « *Réforme du cadre européen de la protection des données à caractère personnel : où en est-on ? »*, Revue Lamy Droit de l'Immatériel 2013 page 99.

MEURIS-GUERRERO, F. « *Une clarification du droit au déréférencement* », Comm. Com. Electr. N°12, Décembre 2015

MEURIS-GUERRERO, F. « *Une clarification du droit au déréférencement et la naissance d'un droit des drones* », Comm. Com. Electr. n°12, décembre 2015.

MORET-BAILLY, J. « *Les modes de définition des professions de santé : présent et avenir*. » RDSS 2008 page 508.

METANILLOS, N. « *Réforme du cadre européen de la protection des données à caractère personnel : où en est on ?* **»** RDLI 2013, n°99, 3303.

NAFTALSKI, F. « *Enjeux et perspectives du pouvoir de labellisation de la Cnil »* Revue Lamy Droit de l'Immatériel, 2010, page 63.

PADOVA, **Y.** « *Le Safe Harbor est invalide. Et après ? Analyse des fondements de l'arrêt de la CJUE et de ses conséquences* », RLDI 2015/120, n° 3867, p. 50-64.

PELLET, R. *« La protection des personnes à l'égard des traitements informatisés des données à caractère médical depuis les ordonnances du 24 avril 1966 »,* RDSS 1996, page 853.

PERRAY, R.

« *Données à caractère personnel, Introduction générale et champ d'application de la loi « Informatique et Libertés* » », J.Cl Comm, fasc, 4710, juillet 2014, spéc. n°25 et s.

« *Informatique, Introduction générale et champ d'application de la loi « Informatique et Libertés »,* J.Cl. Comm, fasc 274-10, mai 2016.

« *Obligations des personnes mettant en œuvre des traitements de données à caractère personnel et droits des personnes concernées »,* J.Cl. Comm. Fasc. 4720, 31 mai 2015.

PIETTE-COUDOL, T. *« L'identité numérique et les identifiants des personnes juridiques »,* Revue Lamy Droit de l'Immatériel - 2013, page 96.

RISSEL, A. *« Les autotests : état des lieux et enjeux »,* RDSS, 2014 page 107.

ROMEYER, **H.** *Tic et santé* Vol. 2, n° 1, 2008.

SAINT-JAMES, V. « *Le droit à la santé dans la jurisprudence du Conseil constitutionnel* », RD publ. 1997, p. 460.

SEGUR, P. « *Confidentialité des données médicales, A propos des enquêtes de santé* », AJDA 2004, p.858.

SOLTANI, S. « *« Big data » et le principe de finalité »,* RLDI 2013/97, n° 3233.

SPITZ, B. « *La révolution du numérique : l'ère de la convergence* », Communication et langages, 1999, n°1, pp. 115-121, Doss. Thém. L'université d'été de la communication.

STEFANI, F. « *Le secret médical à l'épreuve des nouvelles technologies* »**,** Recueil Dalloz 2009. Page 2636.

STEFANI, F. *« Le secret médical à l'épreuve des nouvelles technologies »,* Recueil Dalloz 2009. Page 2636.

THOUVENIN, D. « *La loi relative à la bioéthique ou comment accroître l'accès aux éléments biologiques d'origine humaine* », D. 2005, 116.

TRUDEL, P. Communication du Colloque sur Internet et le Droit, organisé par Paris I, fin 2000.

VACARIE, I. « *L'hébergement des données de santé : entre contrat et statut. »*, RDSS 2002. Page 695.

VARAUT, **J.M.** *«Secret professionnel et confidentialité dans les professions juridiques et judiciaires»,* Gaz. Pal., Rec. 1997, doctr. Page 1054.

VIALLA, F. « *Consentement et Santé sous la direction de l'agence Française de droit de la santé*. », Thème et Commentaire, Bibl Dalloz page 41.

VIVANT, M. « *Comment gérer un traitement de données personnelles ?* », Le Lamy droit du numérique 2016, Guide pratique, n°4233.

VIVANT, M. « *Qu'est-ce qu'être « responsable de traitement ?* », Guide pratique Lamy Droit du numérique 2016, Le Lamy droit des médias et de la communication n°4255**.**

WEINBAUM, N. « Les données personnelles confrontées aux objets connectés »**,** Comm. Com. Electr. N°12, décembre 2014, étude n°22.

Rapports et Avis :

→ *Commission Nationale de l'Informatique et des Libertés*

Avis et Délibérations

De 1980 à1999.

Délibération n°80-016, concernant les traitements automatisés d'informations nominatives relatives à la consommation de gaz, d'électricité, du 6 mai 1980.

Délibération n° 80-10, portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés, du 1er avril 1980.

Délibération n°80-34, relative au traitement automatisé de la comptabilité générale, du 21 octobre 1980.

Délibération n°85-038, relative au paiement du personnel autre que ceux d'un établissement public, du 18 juin 1985,

Délibération n°86-13, portant dénonciation au Parquet de Paris d'infraction à la loi du 6 janvier 1978, 14 janvier 1986

Délibération n°87-102, concernant un projet de décret relatif au fichier automatisé des empreintes digitales géré par le Ministère de l'intérieur, du 14 octobre 1986.

Délibération n°87-100, concernant la réclamation déposée contre la caisse régionale du Crédit Agricole Mutuel d'Ile de France, du 20octobre 1987.

Délibération n°87-106, portant avis sur la mise en place par l'Office Français de Protection des Réfugiées et Apatrides d'un traitement automatisé relatif à la dactyloscopie des demandeurs du statut de réfugié, du 3 novembre 1987.

Délibération n°87-69, portant avis sur la mise en œuvre par la Banque de France d'un traitement automatisé d'informations nominatives relatif à l'information de la Banque de France, des établissements de crédit et des pouvoirs publics sur les agents économiques, du 7 juillet 1987.

Délibération n°88-50, adressant un avertissement à une association gérant « une banque de données d'opposition sur chèques pour le libre usage des particuliers et des commerçants », du 10 mai 1988.

Délibération n°92-032 relative au contrôle effectué le 2 octobre 1992 à la Caisse Régionale de Crédit Agricole de Dordogne, du 6 avril 1993.

Délibération n°93-032 du 6 avril 1993, in 14ième rapport annuel, La Doc. Fr., Collection. Rapports officiels, 1994, page 59.

Délibération n°93-109, relative à la demande d'avis de la CNAMTS concernant le traitement "IRIS", d'échanges d'informations par télétransmission entre organismes complémentaires et caisses primaires d'assurance maladie, du 07 décembre 1993.

Délibération n°94-095, du relative à la proposition modifiée de la directive du Conseil de l'Union Européenne relative à la protection des personnes physiques à l'égard des

traitements des données à caractère personnel et à la libre circulation de ces données, 15 novembre 1994.

Délibération n°97-012, relatives à la segmentation comportementale sur les habitudes comportementales de consommation des ménages, 18 février 1997.

Délibération n°98.041, portant recommandation sur l'utilisation des systèmes de votes par codes-barres dans le cadre d'élections par correspondance pour les élections professionnelles, du 28 avril 1998.

Délibération n°95-144, portant sur une demande d'avis présentée par le Centre de Spectroscopie Nucléaire et de Spectroscopie de Masse d'Orsay concernant un traitement automatisé d'informations nominatives pour la publication d'un annuaire sur un réseau international ouvert, du 7 novembre 1999.

De 2000 à 20009.

Délibération n°01-040, relative à la mission de vérification sur place effectuée auprès de Canal+, du 28 juin 2001.

Délibération n°01-057, portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence, du 29 novembre 2001.

Délibération n° 02-001, ne pouvant concerner que l'entrée et la sortie sur le lieu de travail à l'exception des zones nécessitant un niveau de sécurité particulier Norme simplifiée n°42, du 8 janvier 2002.

Délibération n°02-017, portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opération de recrutement, du 21 mars 2002.

Délibération n°03-034, portant adoption d'une recommandation relative au stockage et à l'utilisation de carte bancaire dans le secteur de la vente à distance, du 19 juin 2003.

Délibération n°03-054, portant avis sur les dispositions relatives au développement de l'administration électronique de l'avant projet de loi habilitant le gouvernement à simplifier le droit par voie d'ordonnance, du 27 novembre 2003.

Délibération n°04-051, portant avertissement à la Caisse d'Epargne des Alpes du 3 juin 2004.

Délibération n° 04-067, modifiée par la délibération n° 2005-126 du 12 mai 2005, Norme simplifiée n°43, du 24 juin 2004, JORF n° 149 du 28 juin 2005.

Délibération n°2005-002, portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels, Norme n°46, du 13 janvier 2005. JORF n°295 du 20 décembre 2005, texte n° 131

Délibération n°2005-038, relative à la modification du traitement « ANAISS » destiné à la gestion des dossiers des usagers des services sociaux des caisses régionales d'assurance maladie et des caisses générale de sécurité sociale, du 10 mars 2005.

Délibération n°2005-213, portant adoption d'une recommandation concernant les modalités d'archivage électronique dans le secteur privé de données à caractère personnel, du 11 octobre 2005.

Délibération n°2005-284, dispensant de déclaration les sites web diffusants ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle, du 22 novembre 2005.

Délibération n°2005-285, portant recommandation sur la mise en œuvre par des particuliers de site web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle, du 22 novembre 2005.

Délibération n°2005-296, du 22 novembre 2005 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet. JORF n°7 du 8 janvier 2006.

Délibération n°2005-296, portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet, du 22 novembre 2005, JORF n°7 du 8 janvier 2006.

Délibération n° 2005-305, portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, du 8 décembre 2005, JORF n° 3 du 4 janvier 2006 page texte n° 79.

Délibération n°2006-056, concernant la dispense de déclaration des traitements mis en œuvre par les collectivités territoriales et les services du représentant de l'Etat dans le cadre de la dématérialisation du contrôle de légalité du 2 mars 2006**.**

Délibération n°2006-103 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire, du 27 avril 2006, AU-009

Délibération n°2006-147, du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés, JORF n°156 du 7 juillet 2006.

Délibération n° 2006-188, portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion du contentieux lié au recouvrement des contraventions au Code de la route et à l'identification des conducteurs dans le cadre du système de contrôle automatisé des infractions au Code de la route, du 6 juillet 2006, JORF n° 45 du 22 février 2007 p n° 122.

Délibération n°2006-218, portant avis sur le projet de décret modifiant le décret no2005-1309 du 20 octobre 2005 pris pour l'application de la loi no78-17 du6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi no2004-801, du 6 août 2004, page 5, du 28 septembre 2006.

Délibération n° 2006-235, portant autorisation unique de mise en œuvre par les organismes de location de véhicules de traitements automatisés de données à caractère personnel ayant pour finalité la gestion de fichiers de personnes à risques, du 9 novembre 2006, JORF n° 297 du 23 décembre 2006.

Délibération n°2006-294, du 21 décembre 2006.

Délibération n° 2007-036, portant avis sur deux projets d'arrêtés relatifs, d'une part, aux spécifications physiques et logiques de la carte d'assurance maladie et aux données y étant contenues et, d'autre part, aux conditions d'émission et de gestion des cartes d'assurance maladie du 20 février 2007.

Délibération n° 2007-326, portant avis sur un projet de décret en Conseil d'Etat modifiant la partie réglementaire du code de procédure pénale et relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAIS) et au casier judiciaire national automatisé, du 8 novembre 2007.

Délibération n° 2007-326, portant avis sur un projet de décret en Conseil d'Etat modifiant la partie réglementaire du code de procédure pénale et relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAIS) et au casier judiciaire national automatisé, du 8 novembre 2007.

Délibération n° 2008-161, du 3 juin 2008, JORF n°0153 du 2 juillet 2008 page texte n° 94.

Délibération n°2008-198, modifiant l'autorisation unique AU-005 relative à certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit. AU 005 du 9 juillet 2008.

Délibération n°2009-148, prononçant une sanction pécuniaire à l'encontre de la société Directannonces, du 26 février 2009.

Délibération n°2009-201, prononçant une sanction pécuniaire de 10 000 Euros à l'encontre de la société JM Philippe, du 16 avril 2009.

Délibération n°2009-203, formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Directannonces, du 26 février 2009**.**

De 2010 à 2016.

Délibération n°2010-028, autorisant la modification de la Banque de France des modalités de gestion du fichier central des retraits des cartes bancaires, du 4 février 2010.

Délibération n°2010-112, décidant de l'interruption d'un traitement vidéo, du 22 avril, 2010.

Délibération n°2010-117, portant avis sur le projet d'arrêté autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Gestion des amendes forfaitaires des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées », du 6 mai 2010.

Délibération n° 2010-460, portant recommandation relative aux conditions de réutilisation des données à caractère personnel contenues dans des documents d'archives publiques, du 9 décembre 2010, JORF n°0026 du 1 février 2011.

Délibération n°2010-449, portant autorisation des traitements de données personnelles mis en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel, du 2 décembre 2010.

Délibération n° 2011-035, prononçant une sanction pécuniaire à l'encontre de la société Google Inc., du 17 mars 2011.

Délibération n° 2011-344, portant avis sur un projet d'arrêté portant création d'un traitement automatisé dénommé « AGRASC » destiné à la gestion et au recouvrement des biens saisis et confisqués par l'Agence de gestion et de recouvrement des avoirs saisis et confisqués, du 10 novembre 2011.

Délibération n° 2011-418, portant avis sur un projet de décret relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle, demande d'avis n° 1523917, du 15 décembre 2011, JORF n°0108.

Délibération n°2011-023, dispensant des traitements automatisés effectués sur le territoire français par des prestataires agissant pour le compte de responsables de traitement établis hors de l'Union européenne et concernant des données personnelles collectées hors de l'Union européenne. (DI-015), du 20 janvier 2011.

Délibération n°2011-035, prononçant une sanction pécuniaire à l'encontre de la société Google inc., du 17 mars 2011.

Délibération n°2011-124, portant avis sur un projet d'arrêté autorisant les traitements de données personnelles dénommés Répertoires Locaux pour les Opérations de Protection des Personnes Agées, du 5 mai 2011.

Délibération n°2011-193, prononçant une sanction à l'encontre de la société PM Participation, dans laquelle elle demande à la société la preuve de l'exécution complète de l'obligation d'information. 28 juin 2011.

Délibération n°2011-203, portant avertissement à l'encontre de la société Pages Jaunes, du 21 septembre 2011.

Délibération n°2011-246, autorisant la mise en œuvre par la société CELTIPharm d'un traitement de données à caractère personnel ayant pour finalité la réalisation d'études épidémiologiques à partir de données issues des feuilles de soins électroniques anonymisées à bref délai, du 8 septembre 2011.

Délibération n°2011-418, portant avis sur un projet de décret relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle, 15 décembre 2011.

2011 Délibération n°2011-423, autorisant la société Geolsementics à mettre en œuvre à titre expérimental, dans le cadre du projet de recherche, les traitements de données à caractère personnel nécessaires au développement d'un outil, dénommé SAIMSI, du 15 décembre 2011.

Délibération n° 2012-084, portant avis sur un projet d'arrêté autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « Fichier national des objectifs en matière de stupéfiants », du 22 mars 2012, (FNOS) NOR: CNIX1231741X.

Délibération n° 2012-209, portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects (Norme simplifiée n° 48), du 21 juin 2012.

Délibération n°2011-384, prononçant une sanction pécuniaire de 20 000 Euros à l'encontre de la société Groupe DES France, du 12 janvier 2012.

Délibération n°2012-061, autorisant l'association HABEO à mettre en œuvre un traitement de données à caractère personnel ayant pour finalité la gestion et le suivi des situations de maltraitance envers les personnes âgées et les adultes handicapés via la mise en place d'une plateforme téléphonique de signalement, Autorisation n°1514929, du 8 mars 2012.

Délibération n°2012-113, portant autorisation unique de traitements de données à caractère personnel contenues dans des informations publiques aux fins de communication et de publication par les services d'archives publiques (décision d'autorisation unique AU-029), du 12 avril 2012.

Délibération n°2012-209, portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs la gestion de clients et de prospects, 21 juin 2012.

Délibération n°2012-213, portant une sanction pécuniaire à l'encontre de la société Equipements Nord Picardie, du 22 juin 2012.

Délibération n°2012-245, autorisant la Cour de Cassation, à mettre en œuvre un traitement de données à caractère personnel ayant pour finalité la constitution de base de jurisprudence Jurinet, du 19 juillet 2012.

Délibération n°2012-404, portant recommandation relative aux traitements des données de consommation détaillées collectées par des compteurs communicants, du 15 novembre 2012.

Délibération n°2012-434, portant avis sur un projet de décision relative au traitement de gestion de la scolarité des étudiants mis à disposition par l'AMUE, 6 décembre 2012.

Délibération 2013-087, portant avis sur un projet d'arrêté relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé GARANCE (Gestion Automatisée de la Rédaction des Actes, des Notes et de la Circulation des Ecrits) - (Demande d'avis n° 1623908), du 28 mars 2013.

Délibération n° 2013-371, autorisant la société Carre Castan Consultants à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la réalisation de veilles et d'études épidémiologiques et médico-économiques à partir des feuilles de résultats d'analyses des laboratoires d'analyses médicales, du 28 novembre 2013.

Délibération n°2013-013, autorisant l'INAVEM à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité le suivi des activités des associations d'aide aux victimes adhérentes et l'établissement de statistiques, du 24 janvier 2013.

Délibération n°2013-091, la CNIL prononce un avertissement à l'encontre de la société Total raffinage marketing, le 11 avril 2013.

Délibération n°2013-105, autorisant l'Institut National des Etudes Démographiques (INED) à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la réalisation et l'analyse des résultats de l'enquête téléphonique réalisée auprès des parents des enfants âgés de deux ans inclus dans la cohorte « Elfe », du 25 avril 2013.

Délibération n°2013-139, prononçant une sanction pécuniaire à l'encontre de la société PS Consulting, du 30 mai 2013.

Délibération n°2013-157, autorisant la mise en œuvre d'un traitement des données à caractère personnel dans un EPAHD dont l'objectif est de faciliter les démarches d'admission des personnes âgées.

Délibération n°2013-210, autorisant la ville de Lyon à effectuer un traitement des données à caractère personnel en matière de sinistre, 11 juillet 2013.

Délibération n°2013-233, autorisant le Crédit Agricole à mettre un traitement de données à caractère personnel pour lutter contre la fraude bancaire, 23 mai 2013.

Délibération n°2013-259, autorisant l'Institut National de la Prévention et de l'Education pour la Santé (INPES) à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité l'étude des caractéristiques socio-économiques des ménages intoxiqués par le monoxyde de carbone de façon accidentelle dans leur habitat et de leur niveau de connaissance quant aux risques d'exposition à ce gaz, 19 septembre 2013, Légifrance.

Délibération n°2013-378, portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978, du 5 décembre 2013, JORF n°0299 du 26 décembre 2013.

Délibération n° 2014-042, modifiant l'autorisation unique n°2005-305 du 8 décembre 2005 n°AU-004 relative aux traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle autorisation unique n°004, du 30 janvier 2014.

Délibération n° 2014-139, autorisant le Conseil Général de la Haute-Marne à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des dossiers traités dans les domaines de l'aide sociale et de l'allocation personnalisée d'autonomie aux personnes âgées, 3 avril 2014.

Délibération n°2014-041, prononçant une sanction pécuniaire à l'encontre de l'association Juricom & Associés, du 29 janvier 2014.

Délibération n° 2015-414, portant avis sur un projet de loi pour une République Numérique, du 19 novembre 2015.

Décision n° 2016-007, mettant en demeure les sociétés Facebook Inc. et Facebook Ireland, du 26 janvier 2016 ; délibération n°2016-026, du bureau de la décidant de rendre publique la mise en demeure n°2016-026, du 4 février 2016.

Délibération n° 2016-005, portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les organismes publics et privés pour la préparation, l'exercice et le suivi de leurs contentieux ainsi que l'exécution des décisions rendues (AU-046), du 14 janvier 2016.

Délibération n°2016-147, portant avis sur le projet de décret en Conseil d'Etat relatif au DMP, du 12 mai 2016.

<u>Rapports CNIL</u>

Avis, 2016-147 portant avis sur un projet de décret pris en Conseil d'Etat relatif au Dossier Bilan d'activité annuel 2015, publié le 8 avril 2016

« Dix ans d'Informatique et Libertés », Economica, 1988, p.36 ; et 8e rapport annuel, la Doc. Fr. Collection. Rapports publics.

« La sécurité de données personnelle », Collection. Guide. Edition 2010.

« Le Quantified self, m-santé : le corps est il un nouvel objet connecté ? »,

Médical Partagé, du 12 mai 2016.

des dispositifs sensibles soumis à autorisation de la CNIL,

Rapport ,17e Rapport, annuel, relatifs aux informations recueillies sur un forum de discussion sur internet, la doc. Fr. Collection. Rapports officiels, 1997, page 92.
Rapport annuel 1979, la Doc. Fr., Collection, Rapports officiels, 1979, p.25.
Rapport annuel 1999, la Doc.fr., Collection, Rapports public, 2000, p.17 à 19
Rapport d'activité 2001, page 157, La Doc. Fr., Collection. Rapports Officiels, 2002.
Rapport sur le droit au déréférencement, « Les critères communs utilisés pour l'examen des plaintes »,2014.
Rapport, 23e Rapport annuel, La Doc. Fr., Collection. Rapports officiels, 2002, page 143.
Rapport, 2e Rapport d'activité, La Doc. Fr. 1978, page 80.
Rapport, 36e rapport annuel d'activité 2015, protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles, Publié le 8 avril 2016
Rapport, 5ième rapport d'activité annuel, la Doc. Fr. Collection. Rapport officiels, 1982, page 131.
Rapport, 6e rapport annuel d'activité 1985 : Doc. fr., 1986, p. 362 ;
Rapport, 7e rapport annuel d'activité 1986 : La Doc. fr., 1987, p. 75.
Rapport, Voix, image et protection des données personnelles, La Doc. Fr., 1996, page 22.

Guides CNIL

Guide « informatique et libertés » pour l'enseignement du second degré, 2010.
Guide du Correspondant Informatique et Libertés, Edition 2011.
Cahiers IP, Vie privée à l'horizon 2020, Cahiers IP n°2, 2012, page 38.
Guide du Big Data, l'annuaire de référence à destination de l'utilisateur, 2014/2015.

Site CNIL

CNIL, Votre ordinateur, publication du 4 janvier 2016.
CNIL, Les listes noires, le fichage des mauvais payeurs et des fraudeurs au regard de la protection des données personnelles, CNIL.2003.
CNIL, Communiqué de presse, 7 avril 2011, relatif à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, Biométrie.
CNIL, Communiqué de presse, du 28 décembre 2007, relatif à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données.

→ ***Groupe de travail de « l'article 29 »***

G29, WP 37, relatif au respect de la vie privée sur internet, §21, adopté le 21 novembre 2000.
G29, Avis 13/2011, WP 185, relatif aux services de géolocalisation des dispositifs mobiles intelligents, adopté le 16 mai 2011.
G29, Avis 10/2004, WP 100, relatif aux dispositions davantage harmonisé en matière d'information, adopté le 25 novembre 2004.

G29, Rapport WP 106, relatif à l'obligation de notification aux autorités nationales de contrôle sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union Européenne, adopté le 18 janvier 2005.
G29, Avis 4/2007, WP 136, relatif au concept de données à caractère personnel, adopté le 20 juin 2007.
G29, Avis 1/2008, sur les aspects de la protection des données liés aux moteurs de recherches, du 4 avril 2008.
G29, Avis 5/2009, WP 163, sur les réseaux sociaux en ligne, adopté le 12 juin 2009.
G29, avis WP 105, relatifs aux questions de protection des données liées à la technologie RFID, 19 janvier 2009 page 9.
G29, Avis 15/2011, WP 187, sur la définition du consentement adopté le 13 juillet 2011.
G29, Avis 5401/01 WP55, concernant la surveillance des communications électroniques sur le lieu de travail, 29 mai 2012.
G29, Avis 05/2012 sur l'informatique en nuage, 1er juillet 2012.
G29, Avis WP 203, concernant la limitation de la finalité, adopté le 2 avril 2013.
G29, Avis « les techniques d'anonymisation » adopté le 10 avril 2014, page 13.
G29, Avis WP 228, « On Surveillance of Electronic Communications for Intelligence and National Security Purposes. », adopté le 5 décembre 2014.
G29, Avis n°2/2010, WP 171, du 22 juin 2010.
G29, Avis 03/2013, WP 203, 2 avril 2013.
G29, Avis 06/2013, WP 207, sur la réutilisation des informations du secteur public (ISP) et des données ouvertes, adopté le 5 juin 2013, page 13.
G29, Avis 05/2014 sur les Techniques d'anonymisation, adopté 10 avril 2014, WP216. Page 8 et 12.
G29, Avis 06/2014, WP 217 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de ladirective95/46/CE, 9 avril 2014.

→ ***<u>Rapports Publics</u>***

ASIP Santé. Cadre d'Interopérabilité des Systèmes d'Information de Santé, 8 décembre 2013.

BOUCHET, **P.** Rapport, La Cybersurveillance des salariés, 2001.

BOURDIN, **J.** Rapport d'information « le commerce électronique, l'irrésistible expansion ».

BRAIBANT, **G.** Rapport au Premier ministre sur la transposition en droit français de la directive numéro 95-46, 3 mars 1998, La Doc. Fr. Collection. Rapports publics.

Comité Consultatif National d'Ethique, Avis n° 76 du 24 avril 2003.

Conseil Consultatif National d'Ethique, Avis n°104 du 29 mai 2008.

Conseil d'Etat, Etude annuelle 2014 du Conseil d'État, La Doc. Fr. Collection. Rapports publics page 156.

Conseil d'Etat, Rapport « Le numérique et les droits fondamentaux », 2014.

Conseil d'Etat, Rapport, « Internet et les réseaux numériques » du 2 juillet 1998.

Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, le 28 janvier 1981, Rapport explication, page 10.

Conseil de l'Ordre des Médecins, Santé Connecté. « De la e-santé à la santé connectée », 31 janvier 2015.

Conseil de l'Ordre des Médecins, sur les dangers des prescriptions par voie électronique, avis du Conseil du 19 août 2000, B.O, n°90, p.13.

Conseil National du Numérique « Rapport sur la neutralité des plateformes, Réunir les conditions d'un environnement numérique ouvert et soutenable » Mai 2014.

Conseil National du Numérique, avis du 30 novembre 2015.

Cour de Cassation. Rapport annuel pour l'année 1999, La Doc. Fr. 2000, page 404.

DETRAIGNE, Y./ ESCOFFIER, A-M., Rapport d'information, « La vie à l'heure des mémoires numériques », 27 mai 2009.

E-HEALTH, Action Plan 2012-2020, 7 décembre 2012.

EVIN, C. / CHARLES, B. / DENIS, J.J. Rapport sur le projet de loi relatif aux droits des malades et à la qualité du système de santé (n° 3258), du 19 septembre 200.

FAGNIEZ, P-L. Rapport au ministre de la santé et des solidarités, Le masquage d'informations par le patient dans son DMP, 30 janvier 2007, La Doc. Fr. 2008, Collection. Rapport Public.

GOUZES, G. Rapport « relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés » page 31.

PERES, E. Conseil Economique, Social et Environnemental, Les données numériques : un enjeu d'éducation et de citoyenneté, Janvier 2015.

PICARD, R. Rapport CGEIET, « Bien Vivre grâce au numérique », février 2012 page 36

TRICOT, B. Rapport rendu sous le nom du rapporteur général M. Bernard Tricot, 27 juin 1975, Le Doc. Fr. Collection. Rapports puclics.

TÜRK, A. Rapport n° 218 (2002-2003) de fait au nom de la commission des lois, déposé le 19 mars 2003.

→ ***Jurisprudences Citées***

Décisions du Conseil Constitutionnel

Conseil Constitutionnel, 23 juillet 1999, n° 99-416 DC, loi portant création d'une couverture maladie universelle, Rec. p. 100 ; AJDA 1999, p. 700, note J.-E. Schoettl.

Conseil Constitutionnel, 10 juin 2009, décision n°2009-580 DC, Loi favorisant la diffusion et la protection de la création sur internat, considérant n°7 ; C. Simon, « les adresses IP sont des données personnelles selon le Conseil Constitutionnel », RLDI 2009, n°59, page 114-115.

Conseil constitutionnel, 10 juin 2009, n° 2009-580 DC, JO 13 juin.

Conseil Constitutionnel, Dec. °2014-412, QPC, M. Lauren « Délit de mise et conservation en mémoire informatisée des données sensibles », Comm. Com. Elec. 2015, obs. A. Debet.

Conseil Constitutionnel, 21 décembre 1999, DEC. n° 99-422, Loi de financement de la sécurité sociale pour 2000, Rec. p. 143 ; AJDA 2000, p. 48, note J.-E. Schoettl.

Conseil d'Etat

CE 11 février 1972, Crochette, recueil Lebon, p. 138

CE, Assemblée 12 mars 1982, n° 25173, publié au recueil Lebon.

CE 31 mai 1989, Mme Roujansky, Lebon, p. 135.

CE 1er juin 1994, CHS Le Valmont, Gaz. Pal. 14-16 juillet 1996, p. 97 Document InterRevues

CE, 7 juin 1995, n°148659, publié au recueil Lebon, Caisse régionale du crédit agricole de Dordogne ; Juris-Data °1995-043340, AJDA 1996, page 162, note J.Frayssinet

CE 6 janvier 1997 n° 159129, Section, Caisse d'Epargne Rhône Alpes Lyon, Publié au recueil Lebon.

CE, 6 janvier 1997, Caisse d'épargne Rhône-Alpes Lyon contre CNIL, n°159129.

CE, 7 octobre 1998, n°186073, publié au recueil Lebon

CE, Ass. 30 juin 2000, Ligue française pour la défense des droits de l'homme, AJDA, , p. 831, concl. P. Fombeur.

CE 13 novembre 2002, n° 234087, Conseil national de l'ordre des médecins.

CE 30 août 2006 n°276 866 AJDA 2006, 1581 ; RTD Civ. 2006 736 obs. M. Hauser.

CE 13 septembre 2006 n°287 530, inédit.

CE, 26 novembre 2006, n°323694, publié au recueil Lebon.

CE, 23 mai 2007, n°288149, inédit, SACEM et Autres.

CE, juge des référés, 19 février 2008 n° 311974, inédit au recueil Lebon

CE, 5 septembre 2008 op. cit. loci.

CE, Juge des référés, 5 septembre 2008, n° 319071, Sté Directannonces : JCP E, 1674 ; Gaz. Pal. 10 octobre 2009 n° 283, p. 5, note G. Haas et L. Goutorbe.

CE, 12 mars 2014, n°353193, publié au recueil Lebon.

CE, 12 mars 2014, n°353193, mentionné au recueil Lebon.

CE, 11 avril 2014, n°355624, Inédit publié au recueil Lebon.

CE, 15 octobre 2014, n°358876 recueil Lebon.

CE, 23 mars 2015, n° 357556, Sté Groupe DES France : JurisData n° 2015-006507.

Cour Cassation

Cass. Civ. 2ième, 17 déc. 1954. 269, note R. Rodiere; JCP 1955. II. 8490 note R.Savatier
Cass crim, 2 novembre 1971, bull crim. N°290.
Cass crim. 7 mars 1973, JCP 197, les grands arrêts en droit de la santé. Dalloz. 2010.
Cass. Crim., 3 novembre 1987, n°87-83429, Bull. Crim. 1987 n° 382 p 1007.
Cass. Crim., 3 novembre 1987, Bull. Crim. n° 382 ; D. 1988, p 17, note H. Maisl.
Cass. Civ. 1re. 24 février 1993, Bull. civ. I n° 87
1995 Cass. Civ. 1ère, 14 nov. 1995, Bull. civ. I, n°414 ; JCP 1996. I. 3985, n°7, obs. G. Viney.
Cass. Crim. 19 décembre 1995, CPII, n°94-81431 : Jurisdata n°1995-004206 ; RJDA 1996/3, °435, obs M. Veron.
Cass. crim., 25 oct. 1995, n° 94-85.781, Bernard X: JurisData n° 1995-003536 ; Bull. Lamy févr. 1996, p. 6.
Cass. Crim. 29 juin 1999, n°97-84166, Bull. Crim. 1999, n°158, JurisData n°1999-003251.
Cass, Soc., n° 98-42.090, 14 mars 2000, D. 2000 IR p 105.
Cass. Civ. 1ère, 20 février 2001, n°99-15970, bull. 2001 I n°43 ; D. 2001 JSP 1199 note J-P Gridel p. 1990, note A. Lepage.
2001 Cass. Civ. juillet 2001, D.2002 jur 1380 note C. Bigot, p. 22298 observation L. Marino.
Cass. crim. 30 octobre 2001, n° 99-82136, inédit.
Cass. Soc. Arrêt « Nikon », 2 octobre 2001, n° 99-42942, Bull. 2001 V n° 291 p233.
Cass. Civ. n°00-19403, 13 novembre 2003, bull. 2003 I n°231 p. 183
Cass. Crim. 16 mars 2004, inédit, n°04-80048.
Cass. Crim. 28 septembre 2004, n°03-86.604 publié au bulletin n°610.
Cour Cass. chbre sociale, 6 avril 2004, n° 01-45227,Gaz. Pal. n°202, 20 juillet 2004, note Joelle Benrenger-Guillon et Laetitia Maurel-Guignot.
Cour de cass. chbre sociale Panorama Dalloz sur la biométrie pour la date de la décision, pan 2004-2005 Dalloz 2005.
CE Section des contentieux, 10ème et 9ème sous-sections réunies, 12 mars 2007 n° 297888, publié au recueil Lebon ; AJDA 2007, p 560.
Cass. Com. 28 novembre 2007, n°06-21964, publié au bulletin, JCP E 2008, n°13, obs, M. Vivant, N. Mallet-Poujol et J-M Bruguière.
Cass. Crim., 20 février 2007, n°06-84310 publié au bulletin crim. n°51.
Cass. Crim. 6 mai 2008, SFR Cegetel, n°07-82.2000, Comm. Com. électr., 2008, n°117, note A. Lepage.
Cass. Civ. 1ère, 12 juillet 2012, n°11-15165 et 11-15188, publié au bulletin, note Hocquet-Berg.
Cass. Civ. 1ière, 10 avril 2013, n°11-19530 publié au Bulletin (Ccass :2013 :C100344)
Cass. com., 25 juin 2013, no 12-17.037, Com. com. électr. 2013, no 9, comm. 90, note Loiseau G., D. 2013, p. 1867, note Beaussonie G., JCP G 2013. 930, p. 1619, note Debet. A., RLDI 2013/96, no 3188, note Varet E. et no 3189, note Mendoza-Caminade A., RLDI 2013/97, no 3222, note Perray R., RLDI 2013/98, no 3248, note Soubelet-Caroit S. et Soubelet L. et no 3264, note Naftalski F. et Colas-Bernie A.-C.
Cass. Civ. 1ère, 10 septembre 2014, n°13-12.464.

Cass. soc., 8 octobre 2014 , n°13-14991, publié au bulletin numérique des chambres civiles.
Cass. 1re civ., 12 mai 2016, n° 15-17.729, M. Stéphane et Pascal X. c/ Les Échos : JurisData n° 2016-008910, com. N. METALLINOS, Comm. Com. Electr. n° 7-8, Juillet 2016, comm. 64.

Cour d'Appel

CA, Versailles, 3 mars 2003, 7eme ch., n° 02/01715.
CA, Besançon 31 janvier 2007, n°RG 06/011896 ; D. 2007, observation A. Lepage
CA, Versailles, 15ième chambre, 11 janvier 2007, R.G. 05-05437, inédit.
CA, Lyon, 17 Mars 2009, n°08/03020.
CA Lyon, 14 avril 2011, affaire n°10/03759 JurisData n°2011-009603.
CA de Dijon, 23 février 2012, n°11/00083, JurisData n°2012-004128.

TGI

TGI de Paris, 5 décembre 1991, Expertises 1992, p.107, note de J. Frayssinet.
TGI Paris 16 déc. 1994. 17e ch. Corr. : Juris data n°1994-600554.
TGI Paris, 22 septembre 2008, Kalid O. contre Notrefamille.com, Note E. Derieux, Legipresse 2008, n°257, §255-10, disponible sur www.legalis.net.
2015 TGI Paris, 23 mars 2015, Comm. Com. Electr. 2015, comm. N°45, obs. A. Debet.

Cour de Justice de l'Union Européenne

CJCE Airey c. Irlande, série affaires n°41, §26, du 9 octobre 1979 ; 13 mai 1980, Artico c. Italie 13 mai 1980.
CJCE, 6 novembre 2003, affaire C-101/01, Bodil Lindqvist, §27.
CJCE, 16 décembre 2008, affaire C-73/07, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy, §37 ; Europe 2009, comm. 54, observations E. Bernard.
CJCE, Productores de Mùsica de España c. Telefònica des España SAU, affaire C-275/06 du 29 janvier 2008.
CJUE, 29 janvier 2008, affaire C-275/06, Promusicae contre Telefonica de Espana.
CJUE, 24 novembre 2011, affaire C70-10, Scarlet Extended SA contre Société belge des auteurs, compositeurs et éditeurs SCRL ; Comm. Com. Electronique 2012, note A. Debet.
CEDH, 18 septembre 2014, affaire n°2010/10, Brunet contre France.
CJUE ; 13 mai 2014, affaire C-131/12, Google Spain SL, Google Inc, C. Agencia Española de Protecciòn de Datos, Mario Costeja Gonzalez, spéc. §28 ; JCP E 2014, 1326, note de M. Griguer et 1327, note G. Busseuil ; A.Debet « Google spain : Un droit l'oubli ou oubli du droit ? », Comm. Com. Electr. 2014, legalis.net.
CJUE, 11 décembre 2014, affaire C-212/13, Riynes, §33.
CJUE, 17 juillet 2014, affaires jointes C-141/12 et C-372/12, YS contre Minister voor Immigratie, Integratie en Asiel et Minister voor Imigratie, Integratie contre M.S.
CJUE, affaire C-131/12, Google spain SL et Google Inc. contre Agencia Española de Protection de datos (AEPD) et Mario Costeja Gonzàlez, 13 mai 2014

2014 CJUE, Affaires jointes C141/12 et C-372/12, Y.S contre Minister voor Immigratie en Asiel et Minister voor Immigratie, Intergratie en Asiel c. M. et S. 17 juillet 2014.
2015 CJUE, affaire n° C-362/14, Maximillian Schrems c Data Protection Commissioner, du 6 octobre 2015

Cour Européenne des Droits de l'Homme
Cour EDH, Leander contre Suède affaire n° 9248/81du 26 mars 1987.
Cour EDH, Rotaru contre Roumanie, du 4 mai 2000 sur les fichiers de systèmisation de la mémorisation des informations des services de renseignements et des pouvoirs publics.
Cour EDH, P.G et J.H. c. Royaume-Uni affaire n° 44787/98, du 25 septembre 2001.
Cour EDH, Odièvre c. France, requête n° 42326/98, du 13 février 2003.
Cour EDH, Perry contre R-U du 17 juillet 2003 affaire n°35829/97 sur l'usage détourné d'un système de vidéo surveillance durant la garde à vue.
Cour EDH, L.L. c. France, requête n° 7508/02, du 10 octobre 2006.
2014 Cour EDH, L.H. c. Lettonie affaire n° 52019/07 du 29 avril 2014.
Cour EDH, Breyer c. Allemagne, requête n° 50001/12, du 21 mars 2016 (requête pendante).

→ ***<u>Webographie :</u>***

« Data brokers : aux Etats- Unis, votre vi privée est en vente », ZDNet.fr, 12 avril 2013.

BIZARD, F. « La vraie bombe de la réforme Touraine : La disparition du secret médical », in Atlantico, 18 mars 2015.

CARBONNIER, **J.** droit civil 1, Thémis n° 71 in Alain LACAMBARATS président de la Chambre de la Cour de cassation. Vie privée et médias. https://www.courdecassation.fr.

DESMARAIS, **P**. « *Dossier médical informatisé* », e-juristes.org, le 5 février 2005.

DESMARAIS, **P**. « *L'impact du numérique sur le consentement du patient* », Consentement et santé, Bibl Dalloz, page 300.

DESMARAIS, **P**. « *réforme de l'hébergement de données de santé: de nouvelles conditions* », 2014.

FIGER, J-P. « *L'informatique en nuage [Cloud Computing], Mode ou révolution ?* », Figer.com, 25 février 2012.

HASSLER, **T**. *« Preuve de l'existence d'un contrat et Internet*», 7 juillet 1999, p. 143, en ligne: Juriscom.net.

HOSPIDROIT, « *établissements de santé, qui est qui ?* ».

L'USINE DIGITALE, « *Données de santé : ce que change la loi du 26 janvier 2016,* » Dossier : Les Big Data, Nouvelle drogue des industries de santé.

LANGLAIS-MPL. - chroniques - « *L'arme de la CNIL : les cases à cocher* » 2013

LAUDE, **A.** *MEDECIN,* Nov- Dèc 2012.

Me. CAPRIOLI, A. « *De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales*», www.uncitral.org/pdf/english/colloquia/EC/Caprioli_Article.pdf

MICHAL-TEITELBAUM, C. « *Secret médical et convention collective : conflits d'intérêt et conflits de loyauté. »,* docteurdu16.blogspot.fr, 2012.

PHARABOD, A-S. « *la mise en chiffre de soi. Une approche compréhensive des mesures personnelles* », Réseaux, n°177, 2013.

SAFINIA, C. PI et TIC, 25 novembre 2004, Legal News.

SEDDIKI, **D.** « *Premiers enseignements du droit à l'oubli* », Droit de l'Homme et Libertés fondamentales, village-justice.com, 1 octobre 2014.

TOPOL, E. « *On the Future of Medicine* » – Wall Street Journal 7 juillet 2014.

TÜRK, A. « *Alex Türk alerte contre les conditions de révision de la Directive de 1995 relative à la protection des données personnelles* », I-MED, Rev. NTIC 2009, n°311

WALTER, J-P. *« Le profilage des individus à l'heure du cyberespace : un défi pour le respect du droit à la protection des données* », Disponible sur www.crid.com

→ ***Liste des sites Internet :***

Agence Régionale de Santé

www.ars.sante.fr

Agence

www.asipsanté.gouv.fr

Cour de Cassation

www.courdecassation.fr

Centre de Recherche et d'Information pour le Développement.

www.crid.asso.fr

Maître Pierre Desmarais

www.desmarais-avocats.fr

Agence des Systèmes d'Information Partagées de Santé

www.esante.gouv.fr

Parlement Européen

www.europarl.europa.eu.

Haute Autorité de Santé

www.has-sante.fr

Ministère de l'Education Nationale et de l'Enseignement Supèrieur

www.horizon2020.gouv.fr

L'hôpital dans le Monde du Droit

www.hospidroit.net

Consiglio Nazionale delle Ricerche

www.ittig.cnr.it

Droit des technologies de l'Information

www.juriscom.net

LexElectronica

www.lex-electronica.org

L'express

www.lexpress.fr

Actualités Informatique et numérique au quotidien

www.nextimpact.com

Agence Nationale de la Sécurité des Système d'Information

www.ssi.gouv.fr

Commission des Nations Unies pour le Droit Commercial International

www.uncitral.org

Annexes

ANNEXE N°1

Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. NIILO JÄÄSKINEN
présentées le 10 juillet 2014[1]

Affaire C-212/13

František Ryneš
contre
Úřad pro ochranu osobních údajů
[demande de décision préjudicielle

formée par le Nejvyšší správní soud (République tchèque)]

«Rapprochement des législations — Traitement des données à caractère personnel — Directive 95/46/CE — Champ d'application — Dérogations — Article 3, paragraphe 2 — Notion d''exercice d'activités exclusivement personnelles ou domestiques' — Enregistrement, par une caméra de surveillance, de l'entrée de la maison de la personne exploitant le système d'enregistrement, de l'espace public ainsi que de l'accès à une maison voisine»

I – Introduction

1. La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2], régit ce domaine d'une manière étendue. Néanmoins, selon son article 3, paragraphe 2, deuxième tiret, ladite directive ne s'applique pas au traitement des données à caractère personnel «effectué par une personne physique pour l'exercice d'activités *exclusivement* personnelles ou domestiques»[3].

2. Le Nejvyšší správní soud (Cour administrative suprême, République tchèque) interroge la Cour sur l'interprétation de cette exception dans le cadre d'un litige opposant M. František Ryneš au Úřad pro ochranu osobních údajů (Office pour la protection des données à caractère personnel, ci-après l'«Office»), au sujet de la décision par laquelle ce dernier a constaté que M. Ryneš avait commis plusieurs infractions dans le domaine de la protection des données à caractère personnel en installant sous la corniche de sa maison une caméra de surveillance qui filmait non seulement sa maison, mais aussi la voie publique et la maison située en face.

3. Sauf erreur de ma part, la Cour n'a jamais eu à connaître d'une affaire dans laquelle elle aurait constaté que les conditions d'application de l'article 3, paragraphe 2, deuxième tiret, de la directive 95/46 étaient réunies, quoique son applicabilité ait été invoquée notamment dans l'affaire Lindqvist[4]. Compte tenu de l'approche qui sous-tend la jurisprudence de la Cour, et notamment les arrêts récents

1 — Langue originale: le français.
2 — JO L 281, p. 31.
3 — Souligné par mes soins.
4 — C-101/01, EU:C:2003:596.

Digital Rights Ireland et Seitlinger e.a.[5] ainsi que Google Spain et Google[6], lesquels font prévaloir le droit fondamental à la protection des données à caractère personnel, je proposerai dans les présentes conclusions de retenir que ladite exception ne couvre pas des situations telles celles visées dans la présente affaire et que, dès lors, la directive 95/46 s'applique.

4. Il convient de souligner que le point de savoir si les activités effectuées par M. Ryneš «afin de protéger les biens, la santé et la vie des propriétaires de la maison» relèvent ou non du champ d'application de la directive 95/46 n'affecte pas dans l'absolu la possibilité d'effectuer une telle surveillance. La présente affaire a pour objet unique de préciser quel est le cadre juridique applicable à cet égard.

II – **Cadre juridique**

A – *Le droit de l'Union*

5. L'article 7 de la charte des droits fondamentaux de l'Union européenne (ci-après la «Charte») dispose que «[t]oute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications».

6. L'article 8, paragraphe 1, de la Charte prévoit que «[t]oute personne a droit à la protection des données à caractère personnel la concernant». Ses paragraphes 2 et 3 donnent les précisions suivantes:

«2. [Les données à caractère personnel] doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante»[7].

7. Les considérants 12 et 16 de la directive 95/46 énoncent:

«(12) [...] doit être exclu le traitement de données effectué par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques, telles la correspondance et la tenue de répertoires d'adresses;

(16) [...] les traitements des données constituées par des sons et des images, tels que ceux de vidéo-surveillance, ne relèvent pas du champ d'application de la présente directive s'ils sont mis en œuvre à des fins de sécurité publique, de défense, de sûreté de l'État ou pour l'exercice des activités de l'État relatives à des domaines du droit pénal ou pour l'exercice d'autres activités qui ne relèvent pas du champ d'application du droit communautaire».

8. L'article 3 de la directive, intitulé «Champ d'application», prévoit:

«1. La présente directive s'applique au traitement des données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé des données à caractère personnel contenues ou appelées à figurer dans un fichier.

5 — C-293/12 et C-594/12, EU:C:2014:238.

6 — C-131/12, EU:C:2014:317.

7 — Selon les explications relatives à cet article, celui-ci «a été fondé sur l'article 286 du traité instituant la Communauté européenne et sur la [directive 95/46], ainsi que sur l'article 8 de la CEDH et sur la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, ratifiée par tous les États membres».

2. La présente directive ne s'applique pas au traitement des données à caractère personnel:

— mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,

— effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.»

B – *La réglementation tchèque*

9. L'article 3, paragraphe 3, de la loi n° 101/2000 Sb., relative à la protection des données à caractère personnel et à la modification de certaines lois (ci-après la «loi n° 101/2000») prévoit:

«la présente loi ne s'applique pas au traitement des données à caractère personnel effectué par une personne physique pour un usage exclusivement personnel».

10. Conformément à l'article 5, paragraphe 2, sous e), de ladite loi, le traitement des données à caractère personnel n'est, en principe, possible qu'avec le consentement de la personne concernée. En l'absence d'un tel consentement, ledit traitement peut avoir lieu s'il s'avère nécessaire à la protection des droits et intérêts protégés par la loi du responsable du traitement, du destinataire ou d'une autre personne concernée. Ce traitement ne doit cependant pas porter atteinte au droit de la personne concernée au respect de sa vie privée et familiale.

11. L'article 44, paragraphe 2, de cette loi régit la responsabilité du responsable du traitement des données à caractère personnel, qui commet une infraction lorsqu'il traite des données à caractère personnel sans le consentement de la personne concernée, lorsqu'il ne fournit pas à la personne concernée les informations pertinentes et lorsqu'il ne satisfait pas à l'obligation de notification à l'autorité compétente.

III – **Le litige au principal, la question préjudicielle et la procédure devant la Cour**

12. Au cours de la période allant du 5 octobre 2007 au 11 avril 2008, M. Ryneš a utilisé une caméra située en dessous de la corniche du toit de sa maison. Elle était fixe, sans possibilité de rotation, et enregistrait l'entrée de sa maison, la voie publique ainsi que l'entrée de la maison située en face. Le système permettait uniquement un enregistrement vidéo, qui était stocké dans un dispositif d'enregistrement continu, à savoir le disque dur. Une fois sa capacité maximale atteinte, il écrasait l'enregistrement existant par un nouvel enregistrement. Le dispositif d'enregistrement ne comportait pas d'écran, de sorte que l'on ne pouvait pas visualiser l'image en temps réel. Seul M. Ryneš avait un accès direct au système et aux données enregistrées.

13. La juridiction de renvoi relève que la seule raison de l'exploitation de cette caméra par M. Ryneš était de protéger les biens, la santé et la vie de celui-ci ainsi que de sa famille. En effet, tant lui-même que sa famille avaient fait l'objet d'attaques pendant plusieurs années de la part d'un inconnu n'ayant pas pu être démasqué. En outre, les fenêtres de la maison, qui appartient à son épouse, ont été brisées à plusieurs reprises entre 2005 et 2007.

14. Au cours de la nuit du 6 au 7 octobre 2007, une fenêtre de la maison de M. Ryneš a été brisée par un tir de projectile au moyen d'une fronde. Grâce au système de vidéosurveillance en cause, deux suspects ont pu être identifiés. Les enregistrements ont été remis à la police et, par la suite, ont été invoqués comme moyen de preuve dans le cadre de la procédure pénale.

15. L'un des suspects a demandé la vérification du système de surveillance de M. Ryneš et l'Office a, par décision du 4 août 2008, constaté que M. Ryneš avait commis des infractions au regard de la loi n° 101/2000 du fait que:

— en tant que responsable du traitement, il avait recueilli, par le biais d'un système de caméra, des données à caractère personnel sans le consentement des personnes se déplaçant dans la rue ou entrant dans la maison située de l'autre côté de la rue,

— les personnes concernées n'avaient pas été informées du traitement de ces données à caractère personnel, de l'étendue et des objectifs de ce traitement, de la personne effectuant le traitement et de la manière dont ledit traitement s'opérait, ni des personnes qui pourraient avoir accès aux données en question,

— en tant que responsable du traitement, M. Ryneš n'avait pas satisfait à l'exigence de notification du traitement en cause à l'Office.

16. Saisi d'un recours formé par M. Ryneš contre cette décision, le Městský soud de Prague l'a rejeté par arrêt du 25 avril 2012. M. Ryneš a formé un pourvoi en cassation contre cet arrêt devant la juridiction de renvoi.

17. Dans ces conditions, par décision du 20 mars 2013, le Nejvyšší správní soud a décidé de surseoir à statuer et de poser à la Cour la question préjudicielle suivante:

«L'exploitation d'un système de caméra installé sur une maison familiale afin de protéger les biens, la santé et la vie des propriétaires de la maison peut-elle relever du traitement des données à caractère personnel 'effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques' au sens de l'article 3, paragraphe 2, de la directive 95/46 [...], même si un tel système surveille également l'espace public?»

18. Des observations écrites ont été déposées par M. Ryneš, par l'Office, par les gouvernements tchèque, espagnol, italien, autrichien, polonais et portugais, par le gouvernement du Royaume-Uni ainsi que par la Commission européenne. Étaient représentés lors de l'audience du 20 mars 2014 l'Office, les gouvernements tchèque, autrichien, polonais et du Royaume-Uni ainsi que la Commission.

IV – **Analyse**

A – *Propos liminaires*

1. Sur les contours de l'affaire

19. Il convient d'observer, premièrement, que, dans la présente affaire, la question préjudicielle est bien précise et se focalise sur l'interprétation de l'expression «pour l'exercice d'activités exclusivement personnelles ou domestiques», dont dépend l'applicabilité de la directive 95/46 à la vidéosurveillance exercée par M. Ryneš. La réponse à cette demande d'interprétation ne peut pas être tributaire du fait

que la vidéosurveillance a abouti à l'objectif recherché, à savoir l'identification des malfaiteurs. La réponse devrait être la même dans l'hypothèse où la vidéosurveillance serait restée infructueuse et n'aurait conduit qu'à des enregistrements, finalement écrasés donc restés inexploités, de personnes se trouvant dans l'espace public devant la maison de M. Ryneš.

20. Deuxièmement, l'affaire porte en substance sur la qualification de la vidéosurveillance en question aux fins de l'application de la directive 95/46. En conséquence, l'usage ultérieur des images enregistrées ne saurait, selon moi, être déterminant pour trancher la question de l'applicabilité même de ladite directive [8]. La qualification juridique de la vidéosurveillance par M. Ryneš ne peut pas varier selon que les images ont été ultérieurement écrasées ou sauvegardées.

21. Troisièmement, l'affaire à l'origine du renvoi préjudiciel se distingue des situations où la vidéosurveillance est exercée par des autorités publiques ou par des personnes morales. En ce qui concerne les autorités publiques, la directive 95/46 est applicable, exception faite des situations visées dans l'article 3, paragraphe 2, première tiret, de cette directive. En ce qui concerne les personnes morales, la directive 95/46 est applicable sans restrictions. C'est pourquoi la jurisprudence de la Cour européenne des droits de l'homme, au demeurant très riche en la matière, ne me semble pas donner d'indications directement transposables [9].

22. Enfin, il apparaît clairement, en l'espèce, que la Charte est applicable, en particulier ses articles 7 et 8. Le cas de figure en question est susceptible de faire naître un conflit entre les droits fondamentaux du responsable du traitement des données (en anglais, «data controller») et ceux de la personne concernée (en anglais, «data subject»). En l'espèce, il s'agit d'un conflit opposant M. Ryneš et les malfaiteurs identifiés. Cependant, dans le contexte de l'applicabilité de la directive 95/46 en général, il s'agit d'un conflit entre le droit à la protection de la vie privée de toute personne physique exerçant une vidéosurveillance d'un espace public et le droit au respect des données à caractère personnel de toute personne concernée s'y trouvant.

23. Si la Cour considère que la directive 95/46 est applicable en l'espèce, il y aurait lieu de procéder à une pondération entre les différents droits et intérêts affectés dans le cadre des dispositions matérielles de ladite directive, et en particulier de son article 7, sous f) [10]. Je tiens à préciser qu'il incomberait, le cas échéant, à la juridiction de renvoi d'y procéder, mais que cela dépasse le cadre défini par le présent renvoi préjudiciel [11].

2. Sur les enseignements jurisprudentiels concernant la protection des données à caractère personnel

24. La directive 95/46 vise à garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel [12].

8 — Si la directive 95/46 est d'application, ledit usage ultérieur de ces données à caractère personnel peut présenter une importance certaine, par exemple en vue d'application de l'article 7, sous f), de cette directive.

9 — Voir, à titre d'exemple de cette jurisprudence, Cour EDH, arrêt Peck c. Royaume-Uni, n° 44647/98, § 57 et jurisprudence citée, CEDH 2003-I.

10 — L'article 7 de ladite directive se lit comme suit: «Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si: […] f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1».

11 — Sur l'application de cette disposition, voir «Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive», disponible en anglais à l'adresse Internet http://ec.europa.eu/justice/data-protection/index_en.htm.

12 — Voir, en ce sens, arrêt IPI (C-473/12, EU:C:2013:715, point 28) ainsi qu'article 1er et considérant 10 de la directive 95/46.

25. La Cour s'inspire de la Charte dans l'interprétation du droit de l'Union. La jurisprudence a également rattaché la directive 95/46 aux principes généraux du droit, et, par ce biais, à l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 [13] (ci-après la «CEDH»). Il a aussi été jugé que la directive 95/46 représente un point d'équilibre, déterminé par le législateur, entre les différents droits fondamentaux en présence [14].

26. Dans l'arrêt Google Spain et Google [15], la Cour a ainsi souligné l'importance de l'effet utile de la directive 95/46 et d'une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques qu'elle vise à assurer [16], notamment le droit au respect de leur vie privée, à l'égard du traitement des données à caractère personnel, auquel cette directive accorde une importance particulière ainsi que le confirment notamment son article 1er, paragraphe 1, et ses considérants 2 et 10 [17].

27. À cet égard, la Cour a déjà dit pour droit que les dispositions de la directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux qui, selon une jurisprudence constante, font partie intégrante des principes généraux du droit dont la Cour assure le respect et qui sont désormais inscrits dans la Charte [18].

28. Plus précisément, dans l'arrêt Google Spain et Google, la Cour a indiqué ce qui suit: «l'article 7 de la Charte garantit le droit au respect de la vie privée, tandis que l'article 8 de la Charte proclame expressément le droit à la protection des données à caractère personnel. Les paragraphes 2 et 3 de ce dernier article précisent que ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi, que toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification et que le respect de ces règles est soumis au contrôle d'une autorité indépendante. Ces exigences sont mises en œuvre notamment par les articles 6, 7, 12, 14 et 28 de la directive 95/46» [19].

29. Je relève que ces dernières dispositions, à l'exception de l'article 28, s'appliquent aussi aux rapports horizontaux entre les responsables du traitement des données qui ne sont pas des autorités publiques et les personnes concernées.

13 — L'article 8, paragraphe 1, de la CEDH est libellé comme suit: «Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance».

14 — Dans l'arrêt Commission/Bavarian Lager (C-28/08 P, EU:C:2010:378, point 63), la Cour a fait prévaloir la protection des données à caractère personnel sur l'accès aux documents en ces termes: «Il s'ensuit que, lorsqu'une demande fondée sur le règlement nº 1049/2001 vise à obtenir l'accès à des documents comprenant des données à caractère personnel, les dispositions du règlement nº 45/2001 deviennent intégralement applicables, y compris les articles 8 et 18 de celui-ci».

15 — EU:C:2014:317, point 58.

16 — Voir, par analogie, arrêt L'Oréal e.a. (C-324/09, EU:C:2011:474, points 62 et 63).

17 — Voir, en ce sens, arrêts Österreichischer Rundfunk e.a. (C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 70); Rijkeboer (C-553/07, EU:C:2009:293, point 47), et IPI (EU:C:2013:715, point 28 et jurisprudence citée).

18 — Voir, notamment, arrêts Google Spain et Google (EU:C:2014:317, point 68); Connolly/Commission (C-274/99 P, EU:C:2001:127, point 37), et Österreichischer Rundfunk e.a. (EU:C:2003:294, point 68).

19 — EU:C:2014:317, point 69.

3. Sur la vidéosurveillance au regard des objectifs de la directive 95/46

a) Sur la vidéosurveillance

30. La vidéosurveillance est caractérisée par son opération permanente et systématique, quelle que soit la durée, variable, de la conservation éventuelle des enregistrements [20]. Je souligne que la présente question préjudicielle porte sur un type de système fixe de surveillance qui s'étend à l'espace public ainsi qu'à la porte de la maison d'en face et permet ainsi d'identifier un nombre indéfini de personnes qui s'y trouvent sans avoir au préalable été averties de ladite surveillance. En revanche, les questions juridiques liées aux enregistrements effectués au moyen de téléphones portables, de caméscopes ou d'appareils photo numériques sont de nature différente, de sorte que les présentes conclusions n'entendent pas les aborder.

31. En effet, le fait qu'une vidéosurveillance avec enregistrement d'images relève du champ de la directive 95/46, dans la mesure où elle constitue en elle-même un traitement automatique (ce qui est le cas dans les enregistrements numériques) ou donne lieu à un tel traitement, résulte d'emblée de son considérant 16.

32. Je note à cet égard que la juridiction de renvoi s'interroge sur l'interprétation de l'article 3, paragraphe 2, deuxième tiret, de la directive 95/46. J'estime dès lors que ladite juridiction considère implicitement, quoique nécessairement, que le traitement en cause dans l'affaire au principal satisfait aux critères établis à l'article 3, paragraphe 1, de ladite directive [21].

33. La juridiction de renvoi ne fournit pas de description détaillée du contenu des enregistrements vidéo en question. Cependant il est permis de penser que, conformément à la jurisprudence de la Cour, des enregistrements de ce type «pris dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci» [22].

34. Par ailleurs, «[l]a conservation des données aux fins de leur accès éventuel par les autorités nationales compétentes», comme cela a été le cas dans l'affaire au principal, «concerne de manière directe et spécifique la vie privée et, ainsi, les droits garantis par l'article 7 de la Charte. En outre, une telle conservation des données relève également de l'article 8 de celle-ci, en raison du fait qu'elle constitue un traitement des données à caractère personnel au sens de cet article et doit, ainsi, nécessairement satisfaire aux exigences de protection des données découlant de cet article» [23].

20 — L'article 29 de la directive 95/46 institue un groupe de travail consultatif indépendant, composé, notamment, des autorités des États membres chargées de la protection des données à caractère personnel (ci-après le «groupe de travail 'Article 29'»). Voir, sur la présente question, l'avis 4/2004 dudit groupe de travail sur le traitement des données à caractère personnel au moyen de la vidéosurveillance, accessible à l'adresse Internet http://ec.europa.eu/justice/data-protection/index_en.htm.

21 — Voir, également, considérant 15 de la directive 95/46, selon lequel «les traitements portant sur de telles données ne sont couverts par la présente directive que s'ils sont automatisés ou si les données sur lesquelles ils portent sont contenues ou sont destinées à être contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause».

22 — Arrêt Digital Rights Ireland et Seitlinger e.a. (EU:C:2014:238, point 27).

23 — Arrêts Digital Rights Ireland et Seitlinger e.a. (EU:C:2014:238, point 29) ainsi que Volker und Markus Schecke et Eifert (C-92/09 et C-93/09, EU:C:2010:662, point 47).

b) Sur les objectifs de la directive 95/46

35. La Cour a indiqué qu'il ressort notamment des troisième, septième et huitième considérants de la directive 95/46 que, en harmonisant des règles nationales protégeant les personnes physiques à l'égard du traitement de données à caractère personnel, cette directive vise principalement à assurer la libre circulation de telles données entre les États membres, qui est nécessaire à l'établissement et au fonctionnement du marché intérieur, au sens de l'article 14, paragraphe 2, CE [24].

36. Conformément à son intitulé, la directive 95/46 répond aussi à un autre objectif, à savoir à la «protection des personnes physiques à l'égard du traitement des données à caractère personnel». La directive crée ainsi un cadre au sein duquel la *protection des personnes physiques* à l'égard du traitement des données à caractère personnel est assurée.

37. Par ailleurs, il est vrai que la libre circulation des données à caractère personnel est susceptible de porter atteinte au droit à la vie privée tel que reconnu notamment à l'article 8 de la CEDH [25] ainsi que par les principes généraux du droit de l'Union [26].

38. Pour cette raison, et ainsi que cela ressort notamment du considérant 10 et de l'article 1er de la directive 95/46, celle-ci vise également à ne pas affaiblir la protection qu'assurent les règles nationales existantes, mais au contraire à garantir, dans l'Union, un niveau élevé de protection des libertés et des droits fondamentaux à l'égard du traitement des données à caractère personnel [27].

39. Il est clair que, s'agissant du droit au respect de la vie privée, «la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire» [28] et que, à cet égard, «la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci» [29].

B – *Sur l'exclusion du champ d'application de la directive 95/46 prévue à l'article 3, paragraphe 2, deuxième tiret*

40. L'affaire au principal soulève la question de savoir si l'activité de M. Ryneš est exclue du champ d'application de la directive 95/46, en application de l'exception prévue à l'article 3, paragraphe 2, deuxième tiret, de la directive 95/46, relative au traitement «effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques». Ladite disposition ne vise pas la finalité du traitement de données à caractère personnel telle que décrite dans la question préjudicielle, à savoir la protection des «biens, [de] la santé et [de] la vie des propriétaires de la maison».

24 — Voir, en ce sens, arrêts Commission/Allemagne (C-518/07, EU:C:2010:125, points 20 à 22) et Österreichischer Rundfunk e.a. (EU:C:2003:294, points 39 et 70).

25 — Voir, en ce sens, Cour EDH, Amann c. Suisse [GC], nº 27798/95, § 69 et 80, CEDH 2000-II, et Rotaru c. Roumanie [GC], nº 28341/95, § 43 et 46, CEDH 2000-V.

26 — Arrêt Commission/Allemagne (EU:C:2010:125, point 21).

27 — Arrêts Commission/Allemagne (EU:C:2010:125, point 22); Österreichischer Rundfunk e.a. (EU:C:2003:294, point 70), ainsi que Satakunnan Markkinapörssi et Satamedia (C-73/07, EU:C:2008:727, point 52).

28 — Arrêts Digital Rights Ireland et Seitlinger e.a. (EU:C:2014:238, point 52) et IPI (EU:C:2013:715, point 39 et jurisprudence citée).

29 — Arrêt Digital Rights Ireland et Seitlinger e.a. (EU:C:2014:238, point 53).

41. Je tiens à préciser que l'affaire au principal ne concerne ni la sûreté de l'État ni des activités de l'État relatives à des domaines du droit pénal, qui pourraient tomber sous l'exception prévue à l'article 3, paragraphe 2, premier tiret, de la directive 95/46, quand bien même les données recueillies en l'espèce ont finalement été transmises aux autorités [30]. En effet, M. Ryneš a agi en tant que personne privée victime d'une infraction pénale, et non en tant qu'agent des forces de l'ordre.

42. M. Ryneš ainsi que les gouvernements tchèque, italien, polonais et du Royaume-Uni sont d'avis que l'exploitation d'un système de vidéosurveillance tel que celui en cause dans l'affaire au principal, qui vise à protéger les biens, la santé et la vie des propriétaires de la maison, est effectuée dans le cadre d'activités exclusivement personnelles ou domestiques au sens de l'article 3, paragraphe 2, deuxième tiret, de la directive 95/46, quand bien même ledit système surveillerait également l'espace public. Au contraire, dans l'hypothèse, comme en l'espèce, où ledit système surveille également l'espace public, l'Office, les gouvernements autrichien, portugais et espagnol ainsi que la Commission estiment que l'exception susmentionnée ne s'applique pas.

a) La prise en compte de la finalité du traitement comme critère d'applicabilité de la directive 95/46

43. Lors de l'audience, la question de savoir si l'application de l'exception pouvait dépendre de l'intention de la personne en cause a été largement abordée. Plus précisément, il s'agit de savoir si le caractère «exclusivement personnel ou domestique» du traitement des données peut être établi au regard de la finalité poursuivie par le responsable du traitement des données.

44. Selon la juridiction de renvoi, M. Ryneš avait procédé à la surveillance «afin de protéger les biens, la santé et la vie des propriétaires de la maison». À mon avis, il n'est pas exclu qu'une activité caractérisée par une telle *finalité subjective* puisse remplir les conditions de l'article 7, sous f), de la directive 95/46, ce qui rendrait le traitement des données à caractère personnel légitime dans le cadre de celle-ci. Ce n'est toutefois pas la question posée à la Cour. La présente question préjudicielle porte sur le champ d'application de la directive 95/46, lequel précède nécessairement toute question relative à l'interprétation de ses dispositions matérielles.

45. Dans ces conditions, il convient de déterminer si le traitement des données à caractère personnel auquel a procédé M. Ryneš échappe au champ d'application de la directive, compte tenu de sa finalité subjective, dans la mesure où cette finalité pourrait être considérée comme constituant un caractère exclusivement personnel ou domestique du traitement des données en question.

46. Je rappelle à cet égard que la fonction de la disposition dans l'article 3, paragraphe 2, deuxième tiret, de la directive 95/46 consiste à définir le champ d'application de ladite directive en excluant certaines situations où une activité, bien que remplissant les critères définis par cette directive, demeure cependant exclue de son champ d'application. Selon moi, le champ d'application d'un instrument du droit de l'Union ne saurait pas dépendre de la finalité subjective de l'intéressé, en l'occurrence du responsable du traitement, dans la mesure où une telle finalité n'est ni objectivement vérifiable sur la base de facteurs externes ni pertinente par rapport aux personnes concernées dont les droits et intérêts sont affectés par l'activité en question.

47. En effet, la finalité du traitement de données à caractère personnel ne saurait être déterminante à l'égard d'un piéton se promenant sur la voie publique et qui fait l'objet d'une vidéosurveillance, du point de vue de son besoin de protection par des dispositions législatives précises définissant sa position juridique par rapport au responsable du traitement des données à caractère personnel. En revanche, la finalité du traitement peut entrer en jeu dans l'appréciation de la licéité de celui-ci. Le champ d'application de la directive doit donc être déterminé au moyen de critères objectifs.

30 — Sur l'exception prévue au premier tiret, voir arrêt Lindqvist (EU:C:2003:596, points 43 et suiv.).

b) Une activité exclusivement domestique ou exclusivement personnelle

48. Pour illustrer le contenu de l'exception en cause, la directive 95/46 mentionne deux exemples: la correspondance et la tenue de répertoires d'adresse [31]. À l'évidence, en tant qu'exception, elle appelle une interprétation restrictive, ce que confirme la jurisprudence portant sur la directive 95/46 [32].

49. En effet, la délimitation très précise de cette exception contribue à empêcher la collecte non réglementée de données à caractère personnel susceptible de s'effectuer en dehors du cadre régi par le droit de l'Union et, par conséquent, exempté des exigences découlant de l'article 8, paragraphes 2 et 3, de la Charte [33].

50. L'affaire Lindqvist, à l'instar de la présente affaire, portait sur le traitement des données à caractère personnel effectué par une personne physique. L'avocat général Tizzano était d'avis que la catégorie des «activités exclusivement personnelles ou domestiques» recouvrait uniquement des activités telles que «la correspondance et la tenue de répertoires d'adresses» […], c'est-à-dire des activités *manifestement* privées et confidentielles, destinées à ne pas sortir de la sphère personnelle ou domestique des intéressés» et que, dans l'affaire en question, l'exception du deuxième tiret n'était pas applicable [34].

51. À mon avis, les «activités personnelles» au titre de l'article 3, paragraphe 2, deuxième tiret, de la directive 95/46, sont des activités étroitement et objectivement liées à la vie privée d'une personne qui ne touchent pas de manière sensible à la sphère personnelle d'autrui. Ces activités peuvent toutefois avoir lieu en dehors du domicile. Les «activités domestiques» sont liées à la vie familiale et ont normalement lieu au sein du domicile ou à d'autres endroits partagés par les membres de la famille, tels qu'une résidence secondaire, une chambre d'hôtel ou une voiture particulière. Elles ont toutes un lien avec la protection de la vie privée prévue à l'article 7 de la Charte.

52. En fait, j'estime à l'instar du gouvernement du Royaume-Uni que cette exception permet dans le cadre juridique actuel, à savoir celui créé par la directive 95/46, d'assurer la protection prévue à l'article 7 de la Charte en faveur de celui qui se livre au traitement de données à caractère personnel dans sa vie privée et familiale.

53. Toutefois, dans le cadre de la directive 95/46, pour que ladite exception puisse jouer, il n'est pas suffisant que les activités envisagées présentent un lien avec des activités personnelles ou domestiques, mais il faut en outre que ce lien soit exclusif. J'ajoute à cet égard que, selon moi, il n'existe aucun doute quant au fait que la condition d'exclusivité s'applique tant aux activités personnelles qu'aux activités domestiques.

54. Je constate que la vidéosurveillance d'autrui, c'est-à-dire une surveillance systématique des lieux moyennant un appareil qui produit un signal vidéo enregistré aux fins de l'identification de personnes, même à l'intérieur d'une maison, ne peut pas être considérée comme *exclusivement personnelle*, mais cela n'exclut pas qu'elle pourrait relever de la notion d'activité domestique.

31 — Considérant 12 de la directive.

32 — Arrêts Satakunnan Markkinapörssi et Satamedia (EU:C:2008:727, points 38 à 49); Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346, points 54 à 61), et Lindqvist (EU:C:2003:596, point 47).

33 — Selon lesdites dispositions, les données à caractère personnel «doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. […] Le respect de ces règles est soumis au contrôle d'une autorité indépendante».

34 — Voir conclusions de l'avocat général Tizzano dans l'affaire Lindqvist (EU:C:2002:513, notamment points 34 et 35, souligné par mes soins). Par ailleurs, il était d'avis que le «traitement en cause est mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire». La Cour a toutefois rejeté cette interprétation.

55. En revanche, il est vrai, comme le soutient le gouvernement du Royaume-Uni, que la protection de l'inviolabilité d'une maison particulière et la protection de celle-ci contre le vol et contre tout accès illicite constituent des activités qui sont essentielles pour chaque ménage et, pour cette raison, peuvent être considérées comme des activités domestiques.

56. Néanmoins, selon moi, une vidéosurveillance qui s'étend à l'espace public ne peut pas être envisagée comme une activité *exclusivement domestique*, parce qu'elle s'étend à des personnes qui n'ont aucun lien avec la famille en question et qui souhaitent conserver leur anonymat. Comme la Cour l'a relevé, «les circonstances que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que» les personnes concernées en l'espèce «en soient informées sont susceptibles de générer dans l'esprit des personnes concernées, […] le sentiment que leur vie privée fait l'objet d'une surveillance constante» [35].

57. Ainsi la vidéosurveillance systématique d'un espace public exercée par les personnes physiques n'est pas exemptée d'exigences dérivées de la protection des données à caractère personnel qui sont applicables à la vidéosurveillance par les personnes morales et les autorités publiques. Cette interprétation permet, au demeurant, de ne pas privilégier les personnes mettant en œuvre une vidéosurveillance d'un espace public situé devant une maison unifamiliale, par rapport à la surveillance qui serait effectuée aux alentours d'autres immeubles en copropriété, car tous les responsables du traitement du données à caractère personnel, personnes physiques ou personnes morales, sont alors soumis aux mêmes exigences [36].

58. J'en conclus qu'un traitement de données à caractère personnel tel que celui effectué par M. Ryneš ne relève pas de la notion d'«exercice d'activités exclusivement personnelles ou domestiques» et ainsi ledit traitement, qui ne bénéficie pas de l'exception en cause, est couvert par le champ d'application de la directive 95/46.

c) Observations complémentaires

59. Afin d'être exhaustif, je tiens à préciser que même si, dans la jurisprudence, la «publication» des données à caractère personnel est souvent mentionnée parmi les éléments retenus pour conclure à l'inapplicabilité de l'exception prévue à l'article 3, paragraphe 2, deuxième tiret, de la directive 95/46 [37], l'absence de publication ne rend pas, a contrario, ladite exception applicable. En effet, l'enregistrement et la conservation des données à caractère personnel constituent en soi une ingérence dans les droits garantis par l'article 7 de la Charte [38].

60. De surcroît, je note que les données à caractère personnel enregistrées par M. Ryneš ont fait l'objet d'une communication aux autorités dans le cadre d'une procédure pénale. À cet égard, il convient de rappeler que, selon la jurisprudence de la Cour, «l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental» [39].

61. Si la Cour retient, comme je le lui propose, que la directive 95/46 est applicable, l'activité exercée par M. Ryneš devra être analysée dans le cadre de ladite directive, laquelle vise à créer et à assurer un équilibre entre les droits fondamentaux et les intérêts des personnes.

35 — Arrêt Digital Rights Ireland et Seitlinger e.a. (EU:C:2014:238, point 37).

36 — Voir avis 4/2004 du groupe de travail «Article 29» sur le traitement des données à caractère personnel au moyen de la vidéosurveillance.

37 — Voir, à titre d'exemple, arrêt Lindqvist (EU:C:2003:596, point 47).

38 — Arrêt Digital Rights Ireland et Seitlinger e.a. (EU:C:2014:238, point 34).

39 — Ibidem (point 35). Voir, en ce qui concerne l'article 8 de la CEDH, Cour EDH, Leander c. Suède, 26 mars 1987, série A n°116, § 48; Rotaru c. Roumanie [GC], n° 28341/95, § 46, CEDH 2000-V, ainsi que Weber et Saravia c. Allemagne (déc.), n° 54934/00, § 79, CEDH 2006-XI.

62. Dans ce cas, il y aura lieu de vérifier notamment la «légitimité» du traitement de données en cause [40]. Sur ce point, il convient de rappeler que, sous réserve des dérogations admises au titre de l'article 13 de la directive 95/46, notamment pour la «protection de la personne concernée ou des droits et libertés d'autrui», tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes relatifs à la qualité des données énoncées à l'article 6 de cette directive et, d'autre part, répondre à l'un des principes relatifs à la légitimation des traitements de données énumérés à l'article 7 de ladite directive [41].

63. Quant à la légitimation d'un traitement tel que celui en cause au principal, je considère que ledit traitement peut bénéficier d'une légitimation visée à l'article 7, sous f), de la directive 95/46.

64. En effet, l'article 7, sous f), de la directive 95/46 prévoit deux conditions cumulatives pour qu'un traitement de données à caractère personnel soit licite, à savoir, d'une part, que le traitement des données à caractère personnel doit être nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées et, d'autre part, que les droits et libertés fondamentaux de la personne concernée ne prévalent pas. Il convient de tenir compte du fait que la seconde de ces conditions nécessite une pondération des droits et intérêts opposés en cause qui dépend, en principe, des circonstances concrètes du cas particulier concerné et dans le cadre de laquelle la personne ou l'institution qui effectue la pondération doit tenir compte de l'importance des droits de la personne concernée résultant des articles 7 et 8 de la Charte [42]. Ledit article 7, sous f), de la directive 95/46 est souvent la clé de voûte pour examiner la légalité du traitement des données à caractère personnel [43].

65. En l'occurrence, il me semble que l'activité exercée par M. Ryneš vise à protéger sa jouissance d'autres droits fondamentaux, tels que le droit de propriété et le droit à la vie familiale.

66. Ainsi, le fait que la directive 95/46 soit applicable n'est pas nécessairement défavorable aux intérêts du responsable du traitement des données à caractère personnel, à condition que ceux-ci soient effectivement légitimes conformément à l'article 7, sous f), de ladite directive. Il n'est pas logique de soutenir que, pour protéger les droits fondamentaux de M. Ryneš, il faudrait laisser inappliquée une directive européenne qui vise précisément à établir un juste équilibre entre les droits de ce dernier et les droits d'autres personnes physiques, à savoir celles qui sont affectées par le traitement de données à caractère personnel.

67. Le fait que la directive 95/46 s'applique à une telle situation n'implique pas, en soi, l'illicéité de l'activité à laquelle s'est livré M. Ryneš. En revanche, c'est dans le cadre de la directive 95/46 qu'il conviendra d'effectuer la pondération entre les droits fondamentaux applicables dans l'affaire au principal.

40 — Sur la légitimation voir, par exemple, arrêt Worten (C-342/12, EU:C:2013:355, points 33 et suiv.).

41 — Arrêts Google Spain et Google (EU:C:2014:317, point 71); Österreichischer Rundfunk e.a. (EU:C:2003:294, point 65); ASNEF et FECEMD (C-468/10 et C-469/10, EU:C:2011:777, point 26), ainsi que Worten (EU:C:2013:355, point 33).

42 — Arrêt ASNEF et FECEMD (EU:C:2011:777, points 38 et 40).

43 — Lors de l'audience, une autre question a été abordée, à savoir l'appréciation à porter sur les caméras embarquées à bord de véhicules enregistreurs. Sur la base de l'interprétation proposée, il me semble clair que ces appareils de surveillance de la voie publique, en ce compris les personnes y circulant, ne peuvent être couverts par ladite exception et que leur utilisation est dès lors pleinement soumise aux conditions prévues par la directive 95/46.

V – **Conclusion**

68. Au vu des considérations qui précèdent, je propose à la Cour de répondre à la question préjudicielle posée par le Nejvyšší správní soud de la manière suivante:

«L'exploitation d'un système de caméra installé sur une maison familiale, afin de protéger les biens, la santé et la vie des propriétaires de la maison qui surveille également l'espace public ne relève pas du traitement des données à caractère personnel effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques au sens de l'article 3, paragraphe 2, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.»

ANNEXE N°2

ICONS	ESSENTIAL INFORMATION	FULFILLED
	No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **processed** for purposes other than the purposes for which they were collected	
	No personal data are **disseminated** to third parties	
	No personal data are **sold or rented out**	
	No personal data are retained in **unencrypted** form	

COMPLIANCE WITH ROWS 1-3 IS REQUIRED BY EU LAW

ANNEXE N°3

Extrait du projet de loi pour une République Numérique

N° 3318

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 9 décembre 2015.

PROJET DE LOI

pour une **République numérique**.

(procédure accélérée)

(Renvoyé à la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement.)

PRÉSENTÉ

AU NOM DE M. Manuel VALLS,
Premier ministre,

PAR M. EMMANUEL MACRON,
ministre de l'économie, de l'industrie et du numérique

ET PAR MME AXELLE LEMAIRE,
secrétaire d'État chargée du numérique

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

Le numérique constitue une nouvelle opportunité de développement, de croissance et de partage pour notre pays, nos entreprises et nos concitoyens. Il est également un formidable moyen de renforcer les valeurs fondamentales de notre République.

À cette fin, le Gouvernement a déjà entrepris des actions de fond, que ce soit par la transformation numérique de l'État ou en matière de politique économique. Il est essentiel de poursuivre cette ambition ; c'est une condition nécessaire du développement du numérique en France sur un rythme aussi soutenu qu'actuellement. L'objectif du Gouvernement est double :

– d'une part, donner une longueur d'avance à la France dans le domaine du numérique en favorisant une politique d'ouverture des données et des connaissances ;

– d'autre part, adopter une approche progressiste du numérique, qui s'appuie sur les individus, pour renforcer leur pouvoir d'agir et leurs droits dans le monde numérique.

Le Gouvernement souhaite ainsi proposer un cadre nouveau, qui combine soutien à l'innovation et aux nouveaux modèles économiques, ouverture élargie des données, protection renforcée des personnes, renforcement de la loyauté des plateformes et déploiement de l'accès au numérique.

Ce cadre a été fixé dans la stratégie numérique du Gouvernement dont le présent projet de loi pour une République numérique constitue le volet législatif. Ce texte a été élaboré à l'issue d'un processus de co-construction innovante au travers d'une grande concertation nationale lancée en octobre 2014 par le Premier ministre au travers de laquelle plus de 4 000 contributions d'entreprises, d'administrations et de particuliers ont été reçues, synthétisées et analysées par le Conseil national du numérique qui a remis au Gouvernement ses conclusions et recommandations le 18 juin dernier.

Un projet de texte a été élaboré par le Gouvernement et a fait l'objet d'une phase de relecture publique sur la plateforme en ligne www.republique-numérique.com du 26 septembre au 18 octobre 2015. Cette plateforme ouverte à tous a suscité plus de 8 500 contributions et près de 150 000 votes.

Le présent projet de loi est enrichi d'une partie des remarques provenant des différents contributeurs que le Gouvernement a jugée utile de prendre en compte.

Il s'organise autour de trois axes :

Favoriser la circulation des données et du savoir :

– renforcer et élargir l'ouverture des données publiques ;

– créer un service public de la donnée ;

– introduire la notion de données d'intérêt général, pour permettre leur réutilisation par tous ;

– développer l'économie du savoir et de la connaissance.

Œuvrer pour la protection des individus dans la société du numérique :

– favoriser un environnement ouvert en affirmant le principe de neutralité des réseaux et de portabilité des données ;

– établir un principe de loyauté des plateformes de services numériques ;

– introduire de nouveaux droits pour les individus dans le monde numérique, en matière de données personnelles et d'accès aux services numériques.

Garantir l'accès au numérique pour tous :

– en favorisant l'accessibilité aux services numériques publics ;

– en facilitant l'accès au numérique par les personnes handicapées ;

– en maintenant la connexion internet pour les personnes les plus démunies.

Le titre I^er^ rassemble les dispositions du projet de loi destinées à favoriser la circulation des données et du savoir.

Le chapitre I^er^ vise à tirer parti de l'économie de la donnée.

La section 1 porte sur l'ouverture des données publiques.

L'ouverture des données publiques a connu dans notre pays deux étapes importantes.

La loi n° 78-753 du 17 juillet 1978 a tout d'abord affirmé une liberté d'accès aux documents administratifs, fondée sur un droit de communication exercé par les administrés sous le contrôle d'une instance spécialisée, la commission d'accès aux documents administratifs (CADA). Les modifications successives apportées à ce texte ont constamment élargi le champ du droit d'accès ainsi reconnu.

L'ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, prise pour la transposition de la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public (dite « directive PSI ») a, dans un deuxième temps, introduit un droit de réutilisation des informations publiques.

Le projet de loi complète le projet de loi relatif à la gratuité et aux modalités de la réutilisation des informations du secteur public, qui met le droit français en conformité avec la directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive PSI de 2003. Cette transposition appelle en réalité très peu de mesures législatives, dans la mesure où la législation française satisfait déjà, sur la plupart des points, aux objectifs assignés par la directive aux États membres.

Le présent projet de loi marque une nouvelle étape dans l'ouverture des données publiques en France. Ses dispositions sont de trois types.

Elles visent en premier lieu à élargir l'accès par internet aux documents administratifs. Cette avancée aura pour conséquence de limiter la communication sur demande des documents administratifs, qui seront rendus librement accessibles par Internet.

En deuxième lieu, le projet de loi énonce le principe selon lequel les informations publiques qui ont été communiquées ou rendues publiques

sont librement réutilisables à d'autres fins que la mission de service public pour laquelle elles ont été produites ou reçues.

En troisième lieu, le projet de loi introduit la notion de données d'intérêt général, en accroissant l'ouverture des données issues de personnes publiques et privées, titulaires de délégations de service public ou dont les activités sont subventionnées par la puissance publique, et en permettant un accès simplifié de la statistique publique à certaines bases de données privées pour des enquêtes statistiques obligatoires.

L'article 1er élargit aux administrations publiques le droit d'accès aux documents administratifs consacré par la loi du 17 juillet 1978. Il crée ainsi une obligation de communiquer les documents détenus par une administration sur demande d'une autre, sous réserve des dispositions des articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration (CRPA), et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

L'article 2 crée un droit d'accès aux règles définissant les traitements algorithmiques utilisés par les administrations publiques et aux principales caractéristiques de leur mise en œuvre, lorsque ces traitements débouchent sur des décisions individuelles.

L'article 3 supprime les dispositions de l'article L. 312-1 du CRPA relatives à la publication de documents administratifs comportant des données personnelles ou des mentions couvertes par les articles L. 311-5 et L. 311-6 : ces dispositions sont remplacées par celles qu'introduit le II de l'article 4.

L'article 4 élargit le champ de la publication obligatoire de documents administratifs, par l'État et les personnes morales de droit public ou de droit privé chargées d'une mission de service public dont le personnel est supérieur à 250. Ce seuil de 250 agents est déjà utilisé pour l'application de dispositions du code de commerce prévoyant l'obligation de rendre publiques certaines informations relatives aux entreprises. Par ailleurs, l'article ne vise que les documents communiqués, sans modifier les exceptions au droit de communication déjà prévues par les articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration : il n'élargit pas le champ des documents communicables mais il modifie leur mode de communication.

Le I crée un nouvel article L. 312-1-1 du CRPA pour rendre obligatoire la publication en ligne par défaut de documents administratifs,

en particulier ceux qui ont déjà été communiqués en vertu du droit d'accès aux documents administratifs garanti par le CRPA, et les bases de données produites ou reçues par les administrations.

Cet article ne modifie pas le régime déjà applicable aux collectivités locales et aux établissements publics de coopération intercommunale à fiscalité propre, introduit dans les dispositions du I et du II de l'article 106 de la loi du 7 août 2015 portant nouvelle organisation territoriale de la République, et consistant en un principe de publication en ligne par défaut pour les collectivités locales de plus de 3500 habitants et leurs intercommunalités.

Le II crée un nouvel article L. 312-1-2 du CPRA, qui fixe les règles pour la publication de documents administratifs comportant des données personnelles ou des mentions couvertes par les articles L. 311-5 et L. 311-6. Pour les documents comportant des données à caractère personnel, leur publication ne sera obligatoire que s'ils ont pu faire l'objet d'un traitement afin de rendre impossible l'identification des personnes concernées.

Une exception à cette publication est également prévue pour ce qui concerne les archives publiques.

L'article 5 modifie en premier lieu l'article L. 311-4 du CRPA pour élargir aux documents publiés en ligne l'obligation de respecter les droits de propriété littéraire et artistique.

Le II prévoit ensuite des mesures transitoires pour l'entrée en vigueur de l'article 4 : des délais de six mois à deux ans sont ménagés pour permettre aux administrations de se préparer aux nouvelles obligations de publication.

L'article 6 élargit le droit de réutilisation des informations publiques en modifiant l'article 10 de la loi du 17 juillet 1978. Il précise que ce droit concerne toutes les informations figurant dans des documents administratifs qui ont été communiqués ou publiés. Il supprime l'exception prévue pour les services publics industriels et commerciaux (SPIC), qui conservent toutefois la possibilité de prévoir des redevances.

L'article 7 du projet de loi comporte diverses dispositions modifiant la loi du 17 juillet 1978.

Le I crée un article 11-1 afin de prévoir une dérogation spécifique au droit *sui generis* du producteur d'une base de données, lorsque ce producteur est une personne publique et qu'il a l'obligation de mettre publiquement en ligne cette base de données.

Le II modifie l'article 16 de la loi du 17 juillet 1978 afin d'encadrer plus strictement les types de licences utilisables par les administrations pour autoriser les réutilisations de données publiques à titre gratuit.

L'article 8 élargit les missions et pouvoirs de la CADA.

Le I prévoit une obligation de mise à jour annuelle du répertoire des principaux documents administratifs que chaque administration doit publier en application de l'article 17 de la loi du 17 juillet 1978.

Le II ouvre la possibilité de saisir la CADA pour avis en cas de refus de publication d'un document administratif. Le III étend la compétence de la CADA au nouveau régime d'accès aux documents administratifs inséré dans le code général des collectivités territoriales par l'article 106 de la loi NOTRe du 6 août 2015.

Le IV rend possible la création d'une procédure simplifiée de réponse aux demandes d'avis reçues par la CADA.

La section 2 traite du service public de la donnée.

L'article 9 crée une nouvelle mission de service public relevant de l'État consistant en la mise à disposition et la publication des données de référence en vue de faciliter leur réutilisation. Les données de référence sont une nouvelle catégorie de données publiques qui sont déjà produites par des autorités administratives pour un objet déterminé (collecte des impôts, statistique publique, etc.) mais qui sont particulièrement importantes pour l'économie et la société en raison des multiples autres usages qui peuvent en être faits.

L'article définit les critères communs à toutes les données de référence, et renvoie aux mesures réglementaires d'application la fixation de la liste précise des données de référence, la désignation des administrations responsables de leur production et de leur diffusion, ainsi que la détermination du niveau minimal de qualité à respecter pour leur diffusion. Le service public de la donnée doit ainsi garantir un niveau de qualité suffisant dans la diffusion de ces données. Le concours des

différentes autorités administratives se traduira par la mise à disposition auprès du service public de la donnée des données qu'elles produisent déjà.

La section 3 traite des données d'intérêt général.

L'article 10 modifie la loi n° 93-122 du 29 janvier 1993 et le code général des collectivités territoriales pour créer une obligation pour un délégataire de missions de service public de remettre à l'autorité délégante les données principales de l'activité gérée en délégation de service public en lui donnant le droit de les publier et d'autoriser leur réutilisation. Il est possible à l'autorité délégante de déroger à cette obligation, à condition que ce soit par une décision motivée et rendue publique.

L'article 11 modifie l'article 10 de la loi n° 2000-321 du 12 avril 2000 pour prévoir une obligation de publication en open data des données essentielles des conventions de subvention, lorsque celles-ci dépassent un seuil déterminé par voie réglementaire (dont le niveau actuel est de 23 000 €).

L'article 12 modifie la loi n° 51-711 du 7 juin 1951 pour permettre à la statistique publique de se voir transmettre sous forme électronique des informations issues de certaines bases de données des personnes enquêtées, dans le seul but de réaliser des enquêtes statistiques obligatoires, et ce afin de simplifier des processus manuels actuels qui sont longs et coûteux. Il prévoit les garanties nécessaires pour protéger les données privées ainsi transmises par les entreprises à la statistique publique. Il crée la possibilité pour le ministre de l'économie de prononcer une amende administrative spécifique en cas de refus de transmission des données concernées.

La section 4 traite de la gouvernance des données.

L'article 13 modifie l'article 13 de la loi n° 78-17 du 6 janvier 1978 pour prévoir que le collège de la Commission nationale de l'informatique et des libertés (CNIL) comprend également le président de la CADA.

L'article 15 modifie symétriquement l'article 23 de la loi n° 78-753 du 17 juillet 1978 pour prévoir que le membre du collège de la CADA désigné par la CNIL est désormais le président de la CNIL ou son représentant.

L'article 14 et l'article 16 prévoient, dans chacune des lois du 6 janvier et du 17 juillet 1978, que les deux commissions peuvent se réunir

dans un collège unique, à l'initiative conjointe du président de la CADA et de celui de la CNIL, lorsqu'un sujet d'intérêt commun le justifie.

Le **chapitre II** a pour objectif de développer l'économie du savoir à travers des mesures portant sur la propriété intellectuelle et sur les travaux de recherche et de statistique.

L'article 17, qui crée un nouvel article L. 533-4 au chapitre III du titre III du livre V du code de la recherche, est relatif à l'accès aux résultats de la recherche publique.

Le monde académique produit un ensemble considérable d'informations, sous la forme de publications scientifiques et de données de toutes natures. L'accès à ces informations et leur réutilisation constituent un enjeu tout à la fois scientifique (partage et mise à jour des connaissances, reproductibilité de la recherche, recherches interdisciplinaires et stimulation des collaborations), économique (opportunités pour l'économie de la connaissance et de l'innovation, notamment pour les PME, rationalisation des moyens consacrés à la recherche, évolution des coûts d'abonnement des bibliothèques aux revues), social et de citoyenneté (participation citoyenne à la recherche, vulgarisation scientifique, éducation, …).

Malgré les possibilités ouvertes par la diffusion numérique, l'accès à ces informations n'est pas aussi aisé qu'on pourrait le souhaiter. Alors qu'il est estimé que la quantité de données générées par la recherche croît au rythme de 30 % chaque année, près de 80 % des données générées au cours des vingt dernières années auraient été perdues, faute de politiques de sauvegarde coordonnées. À côté de ces enjeux, apparaît un risque nouveau de captation de ces données, notamment par des éditeurs scientifiques qui demandent des cessions de licence sur les jeux de données intégrés ou associés aux publications de recherche qu'ils éditent.

Dans ce contexte, l'article 17 vise à favoriser la libre diffusion des résultats de la recherche publique, en cohérence avec les recommandations du 17 juillet 2012 de la Commission européenne relatives à l'accès et la préservation des informations scientifiques, ainsi qu'avec les lignes directrices du programme-cadre de recherche européen Horizon 2020 (2014-2020).

En matière d'accès aux publications scientifiques, l'article retient l'approche équilibrée privilégiée par l'Allemagne qui, sans porter préjudice au droit d'auteur, prévoit depuis le 1er janvier 2014 que le chercheur

dispose d'un « droit d'exploitation secondaire » (« Zweitverwertungsrecht ») sur ses publications.

L'article prévoit ainsi, en son I, que les publications nées d'une activité de recherche financée principalement sur fonds publics peuvent être rendues publiquement et gratuitement accessibles en ligne par leurs auteurs, au terme d'un délai maximum de 6 mois pour les œuvres scientifiques suivant sa première publication, même lorsque l'auteur a accordé des droits exclusifs sur sa publication à un éditeur. Le délai sera de 12 mois pour les œuvres des sciences humaines et sociales, où le temps de retour sur investissement pour les éditeurs est plus long. La réutilisation est libre, à l'exclusion d'une exploitation dans le cadre d'une activité d'édition commerciale, qui pourrait causer un préjudice à l'éditeur. La mise à disposition s'étend à la version finale du texte transmis par l'auteur à l'éditeur avant publication, ainsi qu'à l'ensemble des données de la recherche protégées associées à la publication.

Le II et le III visent à favoriser la diffusion des données de la recherche, tout en reconnaissant leur contribution essentielle au domaine commun de la connaissance. Le II spécifie que la réutilisation de données issues d'activité de recherche financées majoritairement sur des fonds publics est libre, dès lors que ces données ne sont pas protégées par un droit spécifique, comme par exemple un droit de propriété intellectuelle, et qu'elles ont été rendues publiques par le chercheur ou l'organisme de recherche. Le III dispose que la réutilisation des données ne peut être restreinte contractuellement à l'occasion de l'édition d'un écrit scientifique auquel les données seraient associées, lorsque l'écrit a été produit dans le cadre d'une recherche financée principalement sur fonds publics.

L'article 18 modifie l'article 27 de la loi du 6 janvier 1978 pour créer une nouvelle procédure spécifique d'accès à certaines données publiques à des fins statistiques ou de recherche publique. À la place de l'actuel régime d'autorisation par un décret du Conseil d'État en cas de demande d'accès à des données comprenant le numéro de sécurité sociale (NIR), l'article prévoit de substituer un régime de déclaration à la CNIL (pour les travaux de la statistique publique) ou d'autorisation par arrêté après avis de la CNIL (pour les projets de la recherche publique). Cette disposition contribuera à simplifier l'utilisation de ces données aussi bien par les chercheurs que par les agents de la statistique publique dans le cadre de leur mission d'étude ou d'évaluation. Il est prévu qu'un décret en Conseil d'État fixe le cadre de ces nouvelles procédures en définissant les

exigences de chiffrement et d'appariement des bases de données concernées.

Le titre II du projet de loi est consacré à renforcer la protection dans la société numérique. Il s'agit, à travers divers dispositifs destinés à la fois aux citoyens et aux entreprises, de fournir de nouveaux outils de confiance propices aux échanges et à la croissance.

Le chapitre I^{er} crée des dispositions pour un environnement ouvert.

La section 1 traite de la neutralité de l'internet.

Lors de la révision en 2009 du cadre réglementaire européen des communications électroniques « Paquet télécom », de premières mesures ont été adoptées concernant la neutralité des réseaux. Transposées en droit français dans le code des postes et des communications électroniques et dans le code de la consommation par l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, ces mesures s'articulent autour de trois axes :

– le renforcement de la transparence et de l'information des consommateurs concernant les pratiques de gestion de trafic mises en œuvre par les opérateurs de communications électroniques (articles L. 121-83 et L. 121-83-1 du code de la consommation) ;

– la possibilité pour les pouvoirs publics d'intervenir dans les relations entre les opérateurs de communications électroniques et les fournisseurs de services de communication au public en ligne concernant les conditions d'acheminement du trafic (articles L. 32-4 et L. 36-8 du code des postes et des communications) ;

– la garantie du service et la préservation de l'internet dit « best effort » (articles L. 32-1 et L. 36-6 du même code).

Bien qu'elle n'ait pas été saisie de demandes de règlement de différends, l'Autorité de régulation des communications électroniques et des postes (ARCEP) a déjà largement mis en œuvre ses pouvoirs d'enquête. Le recensement des pratiques de gestion de trafic a permis de dissuader les comportements inappropriés si bien que les blocages très répandus auparavant (exemple : blocage de la « VoIP » et du « P2P » sur le mobile) ont totalement disparu. L'Autorité n'a donc pas eu, jusqu'ici, à imposer d'exigences minimales de qualité de service aux opérateurs, mais elle conserve cette possibilité en cas de dégradation constatée de cette

qualité. À cet effet, elle a mis en place un dispositif de mesures qui doit désormais être fiabilisé.

Afin de consolider l'approche harmonisée de la neutralité de l'internet retenue au niveau européen dans le cadre de la proposition de règlement établissant des mesures relatives à l'internet ouvert et modifiant la directive 2002/22/CE sur le service universel et les droits de l'utilisateurs concernant les réseaux de communication et les services et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union (dit « règlement marché unique des télécommunications »), **l'article 19** inscrit au nombre des obligations s'imposant aux exploitants de réseaux ouverts au public et aux fournisseurs de services de communications électroniques le respect des règles portant sur la neutralité de l'internet. L'ARCEP est ainsi directement chargée de veiller au respect du traitement égal et non discriminatoire du trafic par les opérateurs dans les conditions prévues par les articles 3 et 4 du règlement « marché unique des télécommunications » 2015/2120 du 25 novembre 2015. La mise en œuvre par les opérateurs des règles de gestion de trafic prévues par le règlement permettra de garantir un internet libre et ouvert sans pour autant brider les capacités d'innovation de l'ensemble des acteurs du numérique, opérateurs compris.

Par ailleurs, l'article 19 complète les pouvoirs d'enquête administrative de l'ARCEP pour lui permettre d'assurer le contrôle du respect de ces principes. Il est ainsi proposé que les demandes d'informations de l'ARCEP puissent porter non seulement sur l'acheminement mais aussi la gestion du trafic. Ce renforcement des pouvoirs d'enquête de l'ARCEP s'inscrit de plus dans les propositions formulées par le rapport du Conseil général de l'économie et l'Inspection générale des finances sur la fonction économique de l'État.

L'article 20 a pour objectif de permettre à tout utilisateur d'héberger, par les moyens qu'il entend, ses propres données, en utilisant le réseau fourni par l'opérateur de communications électroniques. À cet effet, l'article interdit les mesures techniques visant à empêcher l'utilisateur d'accéder à des données stockées sur un équipement approprié et connecté directement ou indirectement à Internet, *via* le service d'accès auquel il s'est abonné et *via* la « box » dont il dispose.

La section 2 crée un droit à la portabilité des données

L'article 21 a pour objectif principal de réduire la viscosité du marché en obligeant les prestataires de services numériques majeurs, tels que le

courriel et le « cloud computing », à offrir à leurs clients la possibilité de récupérer et transférer leurs données aisément.

La perspective de perdre ses données ou de devoir se lancer dans une récupération manuelle de celles-ci peut en effet inciter le consommateur à renoncer à changer d'opérateur, quand bien même il ne serait plus satisfait de ses services. L'article 18 permet de lever cette barrière et améliorer ainsi le fonctionnement du marché tout en offrant au consommateur une mobilité numérique accrue. Cet article devra être articulé avec le projet de règlement sur les données personnelles en cours de négociation au niveau européen.

Le nouvel article L. 121-121 du code de la consommation, créé par l'article 18, vise à favoriser la portabilité des services de courrier électronique. Il prévoit que l'opérateur de service de courrier électronique offre au consommateur la possibilité de transférer sur un autre service ses courriels, ainsi que sa liste de contacts. Le dernier alinéa étend en outre l'obligation d'accès gratuit au courrier électronique reçu sur l'adresse électronique attribuée sous son nom de domaine durant six mois, qui ne concernait jusqu'à présent que les fournisseurs d'accès à Internet, à tous les opérateurs de services de courrier électronique.

Le nouvel article L. 121-122 du code de la consommation, créé par l'article 18, vise à favoriser la portabilité des données stockées en ligne en instaurant une obligation pour tout fournisseur de service de communication au public en ligne de proposer aux consommateurs une fonctionnalité de récupération des fichiers mis en ligne par le consommateur et des données associées à son compte.

La sous-section 3 a pour objectif d'étendre aux professionnels l'ensemble des dispositions précédentes et de mettre en place des sanctions pour garantir l'effectivité du dispositif.

La section 3 traite de la loyauté des plateformes.

L'étude annuelle du Conseil d'État 2014, intitulée « Numérique et droits fondamentaux », esquisse une définition des plateformes : il s'agit de services de référencement et de classement de contenus fournis par des tiers (par exemple : moteurs de recherche, réseaux sociaux, places de marché…). Il s'agit néanmoins d'intermédiaires actifs, dont le rôle n'est pas neutre. Compte tenu de la puissance acquise par certaines de ces plateformes, des manquements à la législation existante, en particulier en matière de loyauté vis à vis des consommateurs, sont susceptibles d'être relevés.

L'article 22 prévoit à l'article L. 111-5-1 du code de la consommation une définition des opérateurs de plateformes en ligne et impose à ces acteurs nouvellement qualifiés une obligation de loyauté à destination des consommateurs. Cette obligation concerne leurs conditions générales d'utilisation, ou encore leurs modalités de référencement, de classement et de déréférencement des offres mises en ligne.

L'article 22 prévoit également que les plateformes devront faire apparaître clairement l'existence éventuelle d'une relation contractuelle ou de liens capitalistiques avec les personnes référencées, l'existence éventuelle d'une rémunération des personnes référencées et le cas échéant l'impact de celle-ci sur le classement des contenus et des services.

Pour assurer la pleine effectivité de la mise en œuvre des principes de loyauté et de transparence, **l'article 23** encourage les plateformes dont l'audience est importante à définir des bonnes pratiques et des indicateurs de référence et à rendre publique, périodiquement, l'évaluation de leurs propres pratiques. L'article prévoit, par ailleurs, pour réserver la mesure aux principales plateformes, qu'un décret fixera le seuil de connexions au-delà duquel les plateformes en ligne seront soumises à ces obligations.

Afin de répondre aux attentes des parties prenantes et de rechercher une harmonisation des bonnes pratiques, des indicateurs et des informations transmises (et d'en faciliter la comparaison), une concertation sera encouragée entre les plateformes et les pouvoirs publics, les organisations professionnelles, les associations de consommateurs ou d'utilisateurs et toute autre personnalité qualifiée en fonction de ses compétences et de son expérience. La concertation contribuera à l'harmonisation des informations visées au I de l'article et à la définition du format de mise à disposition et de publication des informations, en prévoyant, le cas échéant, l'utilisation d'un standard ouvert aisément réutilisable.

L'article 23 prévoit par ailleurs que l'autorité administrative compétente peut, si elle l'estime nécessaire, publier la liste des plateformes non vertueuses ne respectant par leur obligation et demander toutes informations utiles. Il s'agit par-là de compléter la possibilité de mener les enquêtes et de permettre aux ministres de veiller à la bonne efficacité de la concertation et des initiatives des plateformes.

Cette première étape vise à pouvoir alimenter l'objectivation des pratiques de ces plateformes, et la réflexion, notamment au niveau

européen, sur un éventuel cadre plus contraignant de régulation économique.

L'article 24 introduit une régulation des avis en ligne, qui constitue aujourd'hui une des principales sources d'information des utilisateurs.

L'article L. 111-5-3 introduit dans le code de la consommation une disposition imposant aux sites internet mettant en ligne des avis d'indiquer, de manière explicite, si leur publication a fait l'objet d'un processus de vérification. Elle précise que si le site procède à des vérifications, il est tenu d'en préciser clairement les principales modalités. La mise en place de cette information préalable permettra ainsi au consommateur d'évaluer, par lui-même, le degré de confiance qu'il sera à même d'accorder aux avis mis à sa disposition et, par extension, au site internet qui les publie. Placer ainsi le consommateur en position d'arbitre apparaît être de nature à responsabiliser les responsables de site web dans la mise en ligne des avis et à favoriser un assainissement des pratiques existantes.

En effet, le succès du commerce électronique repose sur deux postulats complémentaires : la sécurité de ce secteur assurée par les professionnels et la confiance accordée par les consommateurs en corollaire. Dans le cadre de ce dernier postulat, la question des avis en ligne tient une place de plus en plus prépondérante. D'après une enquête Nielsen de 2013, 80 % des acheteurs en ligne déclarent tenir compte des avis de consommateurs dans leur démarche d'achat d'un produit ou d'un service et 68 % des répondants font confiance aux opinions postées par d'autres consommateurs. Selon le baromètre 2014 du C2C réalisé par OpinionWay, 74 % des internautes ont d'ailleurs renoncé à un achat en raison d'avis négatifs postés sur l'objet de leur achat.

Or, les enquêtes menées par la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) sur cette thématique ont démontré le développement de la pratique dite des faux avis de consommateurs où un professionnel, directement ou indirectement, pouvait ainsi influer sur l'appréciation des consommateurs sur un produit ou un service, commercialisé ou non par ses soins, ceci pouvant générer *a fortiori* des conséquences non négligeables en matière de loyauté de la concurrence entre professionnels.

La question de la fiabilité des avis en ligne revêt un enjeu clair tant pour le consommateur que pour les entreprises présentes sur internet. Si imposer une vérification systématique des avis serait de nature à créer une contrainte technique et matérielle excessive pour certains sites internet et à

remettre en cause la diversité des sources d'information pour les consommateurs, il n'en demeure pas moins que la confiance du consommateur dans les avis en ligne, et plus largement dans le commerce électronique, doit pouvoir être préservée.

Pour améliorer la transparence et l'information des internautes, l'article 21 prévoit que tout site web qui procède à la collecte et à la publication des avis sur son site indique s'il met en œuvre un processus de vérification des avis déposés et, dans ce cas, décrive le processus mis en place.

L'**article 25** complète les dispositions du code de la consommation par des obligations relatives à l'information contractuelle des consommateurs sur les débits fixes et mobiles. Ces obligations sont prévues par le règlement « marché unique des communications électroniques » 2015/2120 du 25 novembre 2015, dont les dispositions visent à renforcer la transparence sur les pratiques de gestion de trafic, sur la qualité de l'accès à internet. Ces dispositions complètent le cadre européen issu de la directive 2002/22/CE du 7 mars 2002 modifiée dite « directive service universel » en matière d'information contractuelle des utilisateurs de services de communications électroniques transposé à l'article L. 121-83 du code de la consommation.

Le renforcement de l'information des utilisateurs de services de communications électroniques poursuit les efforts déjà engagés par le Gouvernement pour mieux informer les consommateurs sur les débits des offres de communications électroniques (arrêté du 3 décembre 2013 relatif à l'information préalable du consommateur sur les caractéristiques techniques des offres d'accès à l'internet en situation fixe filaire).

L'inscription à l'article L. 121-83 du code de la consommation de ces nouvelles obligations de transparence contractuelle permettra par ailleurs, si nécessaire, d'en préciser les modalités de mise en œuvre par la simple modification de l'arrêté d'application prévu au dernier alinéa de l'article L. 121-83 (arrêté du 16 mars 2006 relatif aux contrats de services de communications électroniques).

Le chapitre II porte sur la protection de la vie privée en ligne.

La section 1 porte sur la protection des données à caractère personnel.

L'article 26 consacre le droit à la libre disposition de ses données, c'est-à-dire le droit de l'individu de décider de contrôler l'usage qui est fait

de ses données à caractère personnel. Il constitue une réponse à la perte de maîtrise par les individus de leurs données personnelles, en donnant sens aux droits déjà reconnus par les textes existants (droit d'accès, droit d'opposition, …).

Cette orientation se distingue de la thèse patrimoniale qui affirme que la meilleure réponse est de faire entrer les données dans le champ patrimonial des personnes. Sauf pour les personnes d'une particulière richesse ou notoriété, la valeur des données personnelles d'un individu est très limitée, de l'ordre de quelques centimes d'euros. C'est le très grand nombre de données traitées qui confèrent leur valeur aux bases manipulées par les acteurs du numérique. Ainsi, le rapport de forces entre le consommateur isolé et l'entreprise, resterait marqué par un déséquilibre structurel. Il est donc préférable de créer un droit rattaché à la personne, à l'image des dispositions équivalentes consacrées par la Cour fédérale allemande.

L'article 27 du projet de loi complète l'article 32 de la « loi informatique et libertés » afin d'ajouter explicitement que la « durée de conservation des catégories de données traitées » fait explicitement partie du périmètre des informations sur lesquelles le droit d'information évoqué supra s'applique.

L'article 28 vise à imposer que, dès lors que le responsable du traitement considéré dispose d'un site internet, les droits d'information, d'opposition, d'accès, et de rectification prévus au chapitre V de la loi « informatique et libertés » puissent être exercés par voie électronique. Cette obligation existe déjà, sans conditions, pour les administrations, en vertu de l'article 4 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Cette disposition est destinée à garantir que l'exercice des droits puisse se faire de manière simple et la plus ergonomique possible. Outre l'intérêt évident pour les citoyens en matière d'exercice de leur droit, le recours à de telle pratique est susceptible de constituer un facteur de réduction de coût et de simplification pour les responsables de traitements.

L'article 29 vise à élargir les missions de la CNIL. Elle jouera dorénavant un rôle plus en amont en soutenant le développement des technologies respectueuses de la vie privée, c'est-à-dire en développant la protection intégrée de la vie privée dès la conception (« Privacy by Design ») et en accompagnant davantage les responsables de traitement.

Le but est également de renforcer son rôle auprès des pouvoirs publics en clarifiant les cas de saisine obligatoire sur les projets de loi et de décret. Enfin, elle pourra conduire une réflexion sur les problèmes éthiques et les questions de société soulevées par l'évolution des technologies.

L'article 30 prévoit que tout responsable de traitement ou sous-traitant peut demander à la Commission nationale de l'informatique et des libertés, au titre de sa mission prévue au *d* du 2° de l'article 11 de la loi du 6 janvier 1978, à bénéficier d'un accompagnement à la mise en conformité des traitements de données à caractère personnel à cette loi. Par ailleurs, il est prévu que la CNIL puisse délivrer des certificats de conformité pour les processus d'anonymisation. Ce dispositif permettra ainsi d'apporter une meilleure sécurité juridique aux porteurs de projets.

Les articles 31 et 32 portent sur la mort numérique et le droit à l'effacement des données pour les mineurs.

S'agissant du droit à l'effacement des données pour les mineurs, le responsable de traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées lorsque la personne concernée était mineure au moment de la collecte. Le projet de loi prévoit pour ce cas de figure une procédure accélérée spécifique avec des délais réduits et une intervention plus rapide de la CNIL. Cet article devra être articulé en coordination avec le projet de règlement européen de protection des données personnelles lorsque celui-ci sera adopté.

L'article 32 est relatif à la gestion des données numériques des personnes décédées. Avec le développement de l'Internet et des réseaux sociaux, les données mises en ligne par les internautes connaissent un fort développement. La gestion de ces données après la mort, soulève des difficultés, les héritiers n'en ayant pas nécessairement connaissance et ne pouvant y avoir accès.

L'article 32 a pour objet de permettre à toute personne, de son vivant, d'organiser les conditions de conservation et de communication de ses données à caractère personnel après son décès. La personne pourra transmettre des directives sur le sort de ses données à caractère personnel à la CNIL ou à un responsable de traitement et pourra désigner une personne chargée de leur exécution.

Par ailleurs, les prestataires sur internet devront informer l'utilisateur du sort de ces données à son décès et lui permettre de choisir de les communiquer ou non à un tiers qu'il désigne. Tout comme l'article 31,

l'article 32 devra être articulé en coordination avec le projet de règlement européen de protection des données personnelles lorsque celui-ci sera adopté.

L'article 33 réforme la procédure de sanction en cas de violation des règles de protection de données à caractère personnel. En cas d'extrême urgence, le délai de mise en demeure par la CNIL pourra être ramené à 24 heures. La sanction pourra même être immédiate lorsque le manquement constaté ne pourra faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure. En cas d'atteinte grave et immédiate aux droits et libertés, le juge pourra en référé ordonner toute mesure nécessaire à la sauvegarde de ces droits et libertés. Enfin, la CNIL pourra décider d'imposer aux responsables de traitements d'informer chaque personne concernée des sanctions qui auront été prononcées à leur encontre. Tout comme les articles 31 et 32, l'article 33 devra être articulé en coordination avec le projet de règlement européen de protection des données personnelles en cours de négociation.

La section 2 traite de la confidentialité des correspondances privées.

L'article 34 est destiné à rappeler et renforcer le respect du principe du secret des correspondances. Le principe du secret des correspondances est un principe essentiel du droit de la communication. Mais à ce jour, la règle du secret des correspondances reste rapportée au seul champ des opérateurs de services de communications électroniques. Or, aujourd'hui, de nombreux services en ligne (services de téléphonie sur IP, réseaux sociaux, services de messagerie en ligne, etc.) sont les supports de correspondances privées. Des évènements récents ont en outre montré que certains de ces services de correspondance en ligne ne respectaient pas le secret des correspondances et entraînaient des atteintes importantes à l'intégrité des correspondances. L'article 34 réaffirme le principe essentiel du secret des correspondances en précisant l'application aux correspondances numériques. L'article précise les cas où des traitements automatisés peuvent analyser le contenu des correspondances (tri, acheminement, anti-spam, anti-virus, services bénéficiant uniquement à l'utilisateur).

Le titre III du projet de loi a pour objectif de renforcer l'accès au numérique.

Le chapitre I^{er} du titre III concerne le numérique et les territoires.

Il est organisé en deux sections. La première porte sur les schémas directeurs territoriaux d'aménagement numérique. La seconde est relative à la couverture du territoire en services de communications électroniques.

Les schémas directeurs territoriaux d'aménagement numérique (SDTAN) prévus à l'article L. 1425-2 du code général des collectivités territoriales « recensent les infrastructures et réseaux de communications électroniques existants, identifient les zones qu'ils desservent et présentent une stratégie de développement de ces réseaux, concernant prioritairement les réseaux à très haut débit fixe et mobile, y compris satellitaire, permettant d'assurer la couverture du territoire concerné. Ces schémas, qui ont une valeur indicative, visent à favoriser la cohérence des initiatives publiques et leur bonne articulation avec l'investissement privé (...) ».

L'élaboration d'un SDTAN constitue un préalable à l'intervention d'une collectivité territoriale en faveur du déploiement du très haut débit sur son territoire. La démarche des SDTAN a connu un grand succès et, au 15 octobre 2014, seuls cinq départements français n'étaient pas concernés par un tel schéma directeur.

L'article 35 du projet de loi a pour objectif d'étendre au domaine des services numériques la démarche des SDTAN en prévoyant que les collectivités territoriales puissent les compléter par un volet relatif à la stratégie de développement des usages et services numériques mis à la disposition des usagers.

Pour inciter la mise en place de grands projets et garantir la cohérence des projets d'implantation des réseaux de communications électroniques à très haut débit sur l'ensemble du territoire, l'**article 36** facilite le regroupement de syndicats mixtes ouverts (SMO) qui ont reçu, de la part des collectivités, la compétence pour développer un réseau de communications électroniques, en autorisant l'adhésion d'un tel SMO à un autre SMO. Cette possibilité est ouverte pour une période limitée dans le temps, s'achevant le 31 décembre 2021.

L'article 37 vise quant à lui au renforcement de la transparence des informations relatives à la couverture du territoire en services de communications électroniques. L'article 33 du projet de loi impose en effet à l'ARCEP de rendre publiques en « *open data* » les données servant notamment à établir les cartes de couverture. Une telle mesure permettra à des tiers d'exploiter ces informations et contribuera in fine à accroître la transparence et à garantir les conditions d'une saine concurrence.

L'article 38 complète les dispositions du code général de la propriété des personnes publiques (CGPPP) dans le but de préciser les éléments à prendre en compte dans le calcul des redevances domaniales dues par un opérateur de communications électroniques. La modification du CGPPP prévoit ainsi qu'outre les avantages de toute nature tirés de l'autorisation d'usage de la ressource domaniale, la redevance tient compte de la nécessité d'assurer la mise en œuvre des technologies permettant l'utilisation la plus efficace des fréquences radioélectriques. L'objectif est que le montant de la redevance contribue à une utilisation optimale du spectre. L'article 34 consacre enfin la gratuité de l'utilisation des fréquences radioélectriques non spécifiquement assignées à leur utilisateur afin d'encourager les projets innovants de partage de fréquences comme le préconise le rapport intitulé « Une gestion dynamique du spectre pour l'innovation et la croissance » remis par Madame Joëlle Tolédano en mars 2014.

L'**article 39** du projet de loi reprend les dispositions de la proposition de loi relative à l'entretien et au renouvellement du réseau des lignes téléphoniques adoptée en première lecture par l'Assemblée nationale. Plus précisément, l'article 35 :

– qualifie l'entretien des réseaux fixes de communications électroniques et de leurs abords d'utilité publique ;

– renforce les obligations de l'opérateur chargé du service universel qui doit dresser un état des lieux détaillé de son réseau fixe avant l'expiration de sa désignation en tant qu'opérateur de service universel ;

– rétablit la servitude d'élagage dont bénéficiait France Télécom et précise la répartition des responsabilités entre les opérateurs exploitant des réseaux et les propriétaires de terrains en matière d'entretien des abords desdits réseaux.

Le chapitre II traite de la facilitation des usages grâce au numérique.

La section 1 porte sur le recommandé électronique.

L'article 40 précise les exigences applicables au recommandé électronique dans le prolongement du règlement européen « eIDAS » ainsi que les modalités de contrôle du respect de ces exigences.

L'article 40 vise ainsi à favoriser le développement des usages en permettant l'utilisation de recommandés sous forme électronique pour tout

type d'échanges. Il vise par ailleurs à renforcer la confiance des usagers en précisant les exigences à respecter par les prestataires de service, afin que le recommandé sous forme électronique apporte les mêmes garanties que le recommandé sous forme papier.

La section 2 porte sur les paiements par SMS.

L'article 41 modifie le régime applicable aux opérations de paiement proposées par un fournisseur de réseaux ou de services de communications électroniques pour l'achat de contenus numériques, de services vocaux ou de tickets ou dans le cadre d'activités caritatives, conforment aux dispositions de la directive sur les services de paiement du 16 novembre 2015. Un des objectifs de ces dispositions est de faciliter la réalisation de dons par SMS. Fortes de leurs valeurs au service de la société civile et afin de développer leurs actions de solidarité, les organisations ont besoins de trouver de nouvelles sources de ressources privées et de nouveaux donateurs. Le don par SMS est une attente forte des organisations bénéficiaires afin de toucher de nouveaux donateurs et mobiliser les citoyens, mais il constitue également une attente des citoyens français et de la société civile car ils sont plus simples, immédiats et s'inscrivent dans les nouvelles pratiques numériques.

L'article 42 est relatif au développement des compétitions de jeux vidéo. Afin de permettre leur développement, il convient d'exempter ces compétitions des interdictions fixées par les articles L. 322-1 à L. 322-2-1 du code de la sécurité intérieure. Cependant, une définition précise et un encadrement des compétitions de jeux vidéo restent nécessaires afin d'éviter toute dérégulation des jeux de cercle électroniques et de prévenir tout risque en termes de santé publique et de lutte contre la fraude et le blanchiment. En vue de définir cet encadrement, l'article habilite le Gouvernement à prendre par ordonnance les mesures relevant du domaine de la loi et modifiant le code de la sécurité intérieure afin de définir le régime particulier applicable aux compétitions de jeux vidéo pour en permettre l'organisation.

Le chapitre III traite de l'accessibilité des publics fragiles au numérique.

La section 1 porte sur l'accessibilité des personnes handicapées aux services téléphoniques.

L'article 43 est destiné à permettre un accès des personnes sourdes et malentendantes aux services téléphoniques, équivalent à celui dont

bénéficient les autres utilisateurs en instaurant une obligation de fourniture d'une traduction écrite simultanée et visuelle en langue française. Cette mise en accessibilité garantira à terme l'autonomie des personnes déficientes auditives pour appeler les services publics ainsi que les services clients des entreprises d'une certaine taille. L'article 39 vise à responsabiliser l'ensemble des acteurs tout en prenant considération les difficultés liées à la rareté de la ressource en interprétariat. L'offre de traduction écrite simultanée et visuelle prévue permettra également d'améliorer l'accès aux services téléphoniques pour une partie des personnes aphasiques.

La section 2 porte sur l'accessibilité des personnes handicapées aux sites internet publics.

L'article 44 crée des obligations à la charge des administrations pour permettre l'accessibilité des sites internet aux personnes handicapées. Ainsi, les sites internet des services de l'État, des collectivités locales et des établissements publics doivent afficher une mention visible permettant de préciser le niveau de conformité ou de non-conformité aux règles d'accessibilité, sous peine de sanction pécuniaire. Le produit issu de ces sanctions sera versé au fonds d'accompagnement de l'accessibilité universelle.

Par ailleurs, ces mêmes administrations doivent élaborer un schéma pluriannuel de mise en accessibilité de leurs sites internet et intranet, de leurs applications mobiles et de leurs progiciels, précisant les modalités de suivi et de contrôle régulier des modifications et changements de contenu. Afin d'assurer le suivi des dispositions de cet article, une commission nationale composée de représentants des personnes visées au premier alinéa de l'article et d'associations représentatives des personnes handicapées pourra être créée.

La section 3 concerne le maintien de la connexion Internet en cas de défaut de paiement.

L'article 45 prévoit le maintien temporaire du service en cas de non-paiement des factures par les personnes les plus démunies. Le service doit être maintenu jusqu'à ce que le fonds de solidarité pour le logement ait statué sur la demande d'aide financière de la personne concernée. Cette disposition est valable pour toute personne ou famille éprouvant des difficultés particulières, au regard notamment de son patrimoine, de l'insuffisance de ses ressources ou de ses conditions d'existence. Il s'agit

d'étendre à l'accès à internet le dispositif existant en matière de fourniture d'électricité, d'eau, de gaz, et de téléphonie fixe.

Le titre IV concerne l'applicabilité du projet de loi dans les collectivités ultramarines relevant d'un régime de spécialité législative.

L'**article 46** comprend les mentions expresses d'application des dispositions du projet de loi en Nouvelle-Calédonie (I), en Polynésie française (II), dans les îles Wallis et Futuna (III) et dans les Terres australes et antarctiques françaises (IV). Dans un souci de lisibilité et d'accessibilité, les dispositions relevant de l'application de plein droit, ont fait l'objet d'une mention expresse d'application pour les distinguer des dispositions qui ne sont pas applicables dans les collectivités concernées. Ce choix résulte aussi du constat que de telles mentions figurent dans nombre de normes modifiées par le projet de loi.

Le titre I^{er} relatif à la circulation des données et du savoir (articles 1er à 18) est entièrement applicable en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna et dans les Terres australes et antarctiques françaises à l'exception des dispositions du II de l'article 10 dans la mesure où elles concernent des dispositions du code général des collectivités territoriales qui ne sont pas applicables dans ces collectivités, ainsi que celles de l'article 12 relatives aux enquêtes statistiques qui ne peuvent être rendues applicables en Nouvelle-Calédonie et en Polynésie française au regard des compétences de ces collectivités.

Le titre II relatif à la protection dans la société numérique (articles 19 à 34) est rendu applicable dans ces mêmes collectivités suivant les dispositions qui leurs sont d'ores et déjà applicables.

Les dispositions relatives à la portabilité et récupération des données (article 21), celles relatives à la loyauté des plateformes (articles 22 et 23) et celles relatives à l'information des consommateurs (article 24) seront uniquement applicables dans les îles Wallis et Futuna. Seule collectivité où les dispositions du code de la consommation ont vocation à s'appliquer, à l'exception de l'article 25 qui porte sur l'article L. 121-83 du code de la consommation qui n'est pas applicable dans cette collectivité en vertu des dispositions de l'article L. 123-1 du même code. La Nouvelle-Calédonie et la Polynésie française sont compétentes en matière de consommation.

Les dispositions relatives à la protection des données à caractère personnel (articles 26 à 33) seront applicables dans l'ensemble des collectivités.

Les dispositions relatives à la confidentialité des correspondances privées (article 34) sont rendues applicables dans les îles Wallis et Futuna. Ces dispositions relèvent de la compétence des collectivités en Nouvelle-Calédonie et en Polynésie française.

Le titre III relatif à l'accès au numérique (articles 35 à 45) est rendu applicable aux collectivités du Pacifique suivant les dispositions qui leurs sont déjà applicables.

Ainsi les dispositions relatives à la compétence et à l'organisation (articles 35 et 36), celles relatives à la couverture numérique (articles 37 à 39), celles relatives au recommandé électronique (article 40) ne sont pas rendues applicables dans ces collectivités parce que les dispositions pertinentes des codes concernés n'y sont pas applicables.

En revanche, les dispositions relatives au paiement par SMS (article 41) y seront applicables.

Seules les dispositions relatives à la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits de l'article 43 relatif à l'accessibilité des personnes handicapées aux services téléphoniques peuvent faire l'objet d'une mention expresse d'application.

Les dispositions relatives à l'accessibilité des personnes handicapées aux sites internet publics (article 44) et au maintien de la connexion internet (article 45) ne font pas l'objet d'une extension d'application en raison de la non application des dispositions visées ou en raison de la compétence des collectivités en la matière.

L'**article 47** procède aux modifications qu'il est nécessaire d'insérer, dans les codes mentionnés par le projet de loi, pour rendre applicables, dans les collectivités du Pacifique, les dispositions nouvelles qu'il créé.

Le code de la consommation est modifié (I) pour l'application des articles 21 à 24 du projet de loi, dans les îles Wallis et Futuna.

Le code de la recherche est modifié (II) pour l'application de l'article 17 du projet de loi, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

Le code des relations entre le public et l'administration (III) pour l'application des articles 2 à 5 et 8 du projet de loi, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

Le code des postes et communications électroniques (IV) pour l'application de l'article 34, dans les îles Wallis et Futuna.

L'**article 48** procède aux modifications qu'il est nécessaire d'insérer, dans les lois mentionnées par le projet de loi, pour rendre applicables, dans les collectivités du Pacifique, les dispositions nouvelles qu'il créé ou modifie :

– à l'article 7 (loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal)

– à l'article 10 (loi n° 93-122 du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques) ;

– à l'article 11 (loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations).

PROJET DE LOI

Le Premier ministre,

Sur le rapport du ministre de l'économie, de l'industrie et du numérique,

Vu l'article 39 de la Constitution,

Décrète :

Le présent projet de loi pour une République numérique, délibéré en conseil des ministres après avis du Conseil d'État, sera présenté à l'Assemblée nationale par le ministre de l'économie, de l'industrie et du numérique, qui sera chargé d'en exposer les motifs et d'en soutenir la discussion, avec le concours de la secrétaire d'État chargée du numérique.

Fait à Paris, le 9 décembre 2015.

Signé : Manuel VALLS

Par le Premier ministre :
Le ministre de l'économie,
de l'industrie et du numérique
Signé : Emmanuel MACRON

La secrétaire d'État chargée du numérique
Signé : Axelle LEMAIRE

TITRE I^ER

LA CIRCULATION DES DONNÉES ET DU SAVOIR

CHAPITRE I^ER

Économie de la donnée

Section 1

Ouverture de l'accès aux données publiques

Article 1^er

Sous réserve des dispositions des articles L. 311-5 et L. 311-6 et sans préjudice des dispositions de l'article L. 114-8 du code des relations entre le public et l'administration, les administrations mentionnées à l'article L. 300-2 du même code sont tenues de communiquer, dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les documents administratifs qu'elles détiennent aux autres administrations mentionnées au même article L. 300-2 qui en font la demande pour l'accomplissement de leurs missions de service public.

Article 2

① Après l'article L. 311-3 du code des relations entre le public et l'administration, il est inséré un article L. 311-3-1 ainsi rédigé :

② « *Art. L. 311-3-1.* – Sous réserve des secrets protégés par les dispositions du 2° de l'article L. 311-5, lorsqu'une décision individuelle est prise sur le fondement d'un traitement algorithmique, les règles définissant ce traitement, ainsi que les principales caractéristiques de sa mise en œuvre, sont communiquées par l'administration à l'intéressé s'il en fait la demande.

③ « Les conditions d'application du présent article sont fixées par décret en Conseil d'État. »

Article 3

Le deuxième alinéa de l'article L. 312-1 du même code est supprimé.

Article 4

① I. – Après l'article L. 312-1 du même code, il est inséré un article L. 312-1-1 ainsi rédigé :

② « *Art. L. 312-1-1.* – Sous réserve des dispositions des articles L. 311-5 et L. 311-6 et lorsque ces documents sont disponibles sous forme électronique, les administrations mentionnées à l'article L. 300-2, à l'exception des personnes morales dont le nombre d'agents ou de salariés est inférieur à deux cent cinquante, rendent publics en ligne, dans un standard ouvert aisément réutilisable, les documents suivants :

③ « 1° Les documents qu'elles communiquent en application des procédures prévues par le présent titre, ainsi que leurs mises à jour ;

④ « 2° L'ensemble des documents qui figurent dans le répertoire mentionné à l'article 17 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal ;

⑤ « 3° Les bases de données qu'elles produisent ou qu'elles reçoivent et qui ne font pas l'objet d'une diffusion publique par ailleurs, ainsi que le contenu de ces bases ;

⑥ « 4° Les données dont l'administration, qui les détient, estime que leur publication présente un intérêt économique, social ou environnemental.

⑦ « Sans préjudice des dispositions de l'article L. 1112-23 du code général des collectivités territoriales et de l'article L. 125-12 du code des communes de Nouvelle-Calédonie, les dispositions du présent article ne s'appliquent pas aux collectivités territoriales, ni aux établissements publics de coopération intercommunale à fiscalité propre auxquels elles appartiennent. »

⑧ II. – Après l'article L. 312-1-1 du même code, il est inséré un article L. 312-1-2 ainsi rédigé :

⑨ « *Art. L. 312-1-2.* – Sauf dispositions législatives ou réglementaires contraires, lorsque les documents visés aux articles L. 312-1 ou L. 312-1-1 comportent des mentions entrant dans le champ d'application des articles L. 311-5 ou L. 311-6, ils ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement afin d'occulter ces mentions.

⑩ « Sauf dispositions législatives ou réglementaires contraires ou si la personne intéressée y a consenti, lorsque les documents visés aux articles L. 312-1 ou L. 312-1-1 comportent des données à caractère personnel, ils ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement afin de rendre impossible l'identification des personnes concernées.

⑪ « Les administrations mentionnées à l'article L. 300-2 ne sont pas tenues de publier les archives publiques issues des opérations de sélection prévues aux articles L. 212-2 et L. 212-3 du code du patrimoine. »

⑫ III. – Un décret en Conseil d'État, pris après avis de la commission mentionnée au titre IV, définit les modalités d'application des articles L. 312-1 à L. 312-1-2.

Article 5

① I. – À l'article L. 311-4 du même code, après les mots : « sont communiqués », sont insérés les mots : « ou publiés ».

② II. – Sans préjudice des dispositions de l'article L. 1112-23 du code général des collectivités territoriales et de l'article L. 125-12 du code des communes de Nouvelle-Calédonie :

③ 1° Dans un délai de six mois à compter de la publication de la présente loi, les administrations mentionnées à l'article L. 312-1-1 du code des relations entre le public et l'administration publient les documents qu'elles communiquent en application des procédures prévues par le titre I^{er} du livre III du même code ;

④ 2° Dans un délai d'un an à compter de la publication de la présente loi, les administrations mentionnées à l'article L. 312-1-1 du même code publient l'ensemble des documents qui figurent dans le répertoire mentionné à l'article 17 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal ;

⑤ 3° À une date fixée par décret et au plus tard deux ans après la publication de la présente loi, les administrations mentionnées à l'article L. 312-1-1 du même code publient l'ensemble des documents et dans les conditions précisés à ce même article.

Article 6

① L'article 10 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal est remplacé par les dispositions suivantes est ainsi modifié :

② 1° Le premier alinéa est ainsi rédigé :

③ « Les informations publiques figurant dans des documents administratifs communiqués ou publiés peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus. Les limites et conditions de cette réutilisation sont régies par le présent chapitre. Lorsqu'elles sont mises à disposition sous forme électronique, ces informations le sont, si possible, dans un standard ouvert et aisément réutilisable, c'est-à-dire lisible par une machine. » ;

④ 2° Le *b* est abrogé. Le *c* devient le *b ;*

⑤ 3° Au dernier alinéa, l'expression : « article 1er » est remplacée par l'expression : « article L. 300-2 du code des relations entre le public et l'administration ».

Article 7

① I. – Après l'article 11 de la loi du 17 juillet 1978 précitée, il est inséré un article 11-1 ainsi rédigé :

② « *Art. 11-1.* – Sous réserve de droits de propriété intellectuelle détenus par des tiers, les droits des administrations mentionnées à l'article L. 300-2 du code des relations entre le public et l'administration, au titre des articles L. 342-1 et L. 342-2 du code de la propriété intellectuelle, ne peuvent faire obstacle à la réutilisation, au sens de l'article 10, du contenu des bases de données que ces administrations ont obligation de publier en application du 3° de l'article L. 312-1-1 du code des relations entre le public et l'administration. »

③ II. – L'article 16 est complété par un alinéa ainsi rédigé :

④ « Lorsque les réutilisations à titre gratuit donnent lieu à l'établissement d'une licence, cette licence est choisie parmi celles figurant sur une liste fixée par décret. Lorsqu'une administration souhaite recourir à une licence

ne figurant pas sur cette liste, cette licence doit être préalablement homologuée par l'État, dans des conditions fixées par décret. »

Article 8

① I. – Le premier alinéa de l'article 17 de la loi du 17 juillet 1978 précitée est complété par une phrase ainsi rédigée : « Elles publient chaque année une version mise à jour de ce répertoire. »

② II. – À l'article L. 342-1 du code des relations entre le public et l'administration, après les mots : « refus de communication » sont insérés les mots : « ou un refus de publication ».

③ III. – Au 3° du A de l'article L. 342-2 du même code, après les mots : « Les articles » est insérée la référence : « L. 1112-23, ».

④ IV. – Au dernier alinéa de l'article L. 341-1 du même code, après les mots : « délibérer en formation restreinte » sont insérés les mots : « ou déléguer à son président l'exercice de certaines de ses attributions ».

Article 9

① La mise à disposition et la publication des données de référence en vue de faciliter leur réutilisation constituent une mission de service public relevant de l'État. Toutes les autorités administratives concourent à cette mission.

② Sont des données de référence les données produites ou reçues par les administrations mentionnées à l'article L. 300-2 du code des relations entre le public et l'administration qui font l'objet ou sont susceptibles de faire l'objet d'utilisations fréquentes par un grand nombre d'acteurs tant publics que privés et dont la qualité, en termes notamment de précision, de fréquence de mise à jour ou d'accessibilité, est essentielle pour ces utilisations. Un décret fixe la liste des données de référence et désigne les administrations responsables de leur production et de leur publication.

③ Les modalités d'application du présent article sont définies par un décret en Conseil d'État. Dans l'hypothèse où plusieurs administrations sont responsables, le décret détermine les modalités de la coordination entre ces administrations. Il fixe la qualité minimale que la publication des données de référence doit respecter, notamment en termes de précision, de degré de détail, de fréquence de mise à jour, d'accessibilité et de format. Il

précise les modalités de participation des collectivités territoriales à la mise à disposition et à la publication des données de référence.

Section 2

Données d'intérêt général

Article 10

① I. – Dans la loi n° 93-122 du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques, il est inséré un article 40-2 ainsi rédigé :

② « *Art. 40-2.* – Le délégataire fournit à la personne morale de droit public, dans un standard ouvert aisément réutilisable, les données et bases de données collectées ou produites à l'occasion de l'exploitation du service public. Il autorise par ailleurs la personne morale de droit public, ou un tiers désigné par celle-ci, à extraire et exploiter librement tout ou partie de ces données et bases de données, notamment en vue de leur mise à disposition à titre gratuit à des fins de réutilisation à titre gratuit ou onéreux.

③ « La personne morale de droit public peut exempter le délégataire des obligations prévues au premier alinéa par une décision motivée et rendue publique. »

④ II. – Après l'article L. 1411-3 du code général des collectivités territoriales, il est inséré un article ainsi rédigé :

⑤ « *Art. L. 1411-3-1.* – Le délégataire fournit à la personne morale de droit public, dans un standard ouvert aisément réutilisable, les données et bases de données collectées ou produites à l'occasion de l'exécution du service public. Il autorise par ailleurs la personne morale de droit public, ou un tiers désigné par celle-ci, à extraire et exploiter librement tout ou partie de ces données et bases de données, notamment en vue de leur mise à disposition à titre gratuit à des fins de réutilisation à titre gratuit ou onéreux.

⑥ « La personne morale de droit public peut exempter le délégataire des obligations prévues au premier alinéa par une décision motivée et rendue publique. »

⑦ III. – Les I et II du présent article sont applicables aux contrats conclus ou reconduits postérieurement à la promulgation de la présente loi.

Article 11

① L'article 10 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations est ainsi modifié :

② 1° Au cinquième alinéa, les mots : « le seuil mentionné au troisième alinéa » sont remplacés par les mots : « le seuil mentionné au quatrième alinéa » ;

③ 2° Il est inséré un huitième alinéa ainsi rédigé :

④ « L'autorité administrative ou l'organisme chargé de la gestion d'un service public industriel et commercial mentionné au premier alinéa de l'article 9-1 qui attribue une subvention dépassant le seuil mentionné au quatrième alinéa du présent article rend accessible, sous un standard ouvert aisément réutilisable, les données essentielles de la convention de subvention, dans des conditions fixées par voie règlementaire. »

Article 12

① La loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques est ainsi modifiée :

② 1° Le second alinéa de l'article 3 est supprimé ;

③ 2° Il est inséré un article 3-1 ainsi rédigé :

④ *« Art. 3-1.* – I. – Le ministre chargé de l'économie peut décider, après avis du Conseil national de l'information statistique, que les personnes morales de droit privé sollicitées pour des enquêtes transmettent par voie électronique au service statistique public à des fins exclusives d'établissement de statistiques les informations présentes dans les bases de données qu'elles détiennent lorsque ces informations sont recherchées pour les besoins d'enquêtes statistiques qui sont rendues obligatoires en vertu de l'article 1er *bis*.

⑤ « Cette décision est précédée d'une étude de faisabilité et d'opportunité rendue publique. »

⑥ « Les données transmises par les personnes morales de droit privé sollicitées pour ces enquêtes ne peuvent être communiquées à quiconque. Seules sont soumises aux dispositions du livre II du code du patrimoine les informations issues de ces données ayant été agrégées et ne permettant pas l'identification de la personne morale enquêtée.

⑦ « Les conditions dans lesquelles sont réalisées ces enquêtes, notamment leur faisabilité, leur opportunité, les modalités de collecte des données de même que, le cas échéant, celles de leur enregistrement temporaire, font l'objet d'une concertation avec les personnes morales sollicitées pour l'enquête et sont fixées par voie réglementaire.

⑧ « II. – Par dérogation aux dispositions de l'article 7, en cas de refus de la personne morale sollicitée pour l'enquête de procéder à la transmission d'informations conformément à la décision prise dans les conditions mentionnées au I, le ministre chargé de l'économie met en demeure la personne enquêtée. Cette mise en demeure fixe le délai imparti à la personne sollicitée pour l'enquête pour faire valoir ses observations. Ce délai ne peut être inférieur à un mois.

⑨ « Si la personne sollicitée pour l'enquête ne se conforme pas à cette mise en demeure, le ministre saisit pour avis le conseil national de l'information statistique réuni en comité du contentieux des enquêtes statistiques obligatoires. La personne sollicitée pour l'enquête est entendue par le comité.

⑩ « Au vu de cet avis, le ministre peut, par une décision motivée, prononcer une amende administrative.

⑪ « Le montant de la première amende encourue à ce titre ne peut dépasser 25 000 €. En cas de récidive dans un délai de trois ans, le montant de l'amende peut être porté à 50 000 € au plus.

⑫ « Le ministre peut rendre publiques les sanctions qu'il prononce. Il peut également ordonner leur insertion dans des publications, journaux et supports qu'il désigne aux frais des personnes sanctionnées. »

Section 3

Gouvernance

Article 13

① L'article 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi modifié :

② 1° Au premier alinéa, le mot : « dix-sept » est remplacé par le mot : « dix-huit » ;

③ 2° Après le 7°, il est inséré un alinéa ainsi rédigé :

④ « 8° Le président de la commission d'accès aux documents administratifs, ou son représentant. »

Article 14

① Il est ajouté à la même loi un article 15 *bis* ainsi rédigé :

② « *Art. 15 bis.* – La Commission nationale de l'informatique et des libertés et la commission d'accès aux documents administratifs se réunissent dans un collège unique, sur l'initiative conjointe de leurs présidents, lorsqu'un sujet d'intérêt commun le justifie. »

Article 15

① Le septième alinéa de l'article 23 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal est remplacé par un alinéa ainsi rédigé :

② « *f)* Le président de la Commission nationale de l'informatique et des libertés ou son représentant. »

Article 16

① Il est ajouté à la même loi un article 23 *bis* ainsi rédigé :

② « *Art. 23 bis.* – La commission d'accès aux documents administratifs et la Commission nationale de l'informatique et des libertés se réunissent

dans un collège unique, sur l'initiative conjointe de leurs présidents, lorsqu'un sujet d'intérêt commun le justifie. »

CHAPITRE II

Économie du savoir

Article 17

① À la fin du chapitre III du titre III du livre V du code de la recherche, il est ajouté un article L. 533-4 ainsi rédigé :

② « *Art. L. 533-4.* – I. – Lorsqu'un écrit scientifique, issu d'une activité de recherche financée au moins pour moitié par des dotations de l'État, des collectivités territoriales ou des établissements publics, par des subventions d'agences de financement nationales ou par des fonds de l'Union européenne, est publié dans un périodique paraissant au moins une fois par an, dans des actes de congrès ou de colloques ou des recueils de mélanges, son auteur dispose, même en cas de cession exclusive à un éditeur, du droit de mettre à disposition gratuitement sous une forme numérique, sous réserve des droits des éventuels coauteurs, la version finale du manuscrit acceptée pour publication, dès lors que l'éditeur met lui-même l'écrit gratuitement à disposition sous une forme numérique, et, à défaut, à l'expiration d'un délai courant à compter de la date de la première publication. Ce délai est de six mois pour les sciences, la technique et la médecine, et de douze mois pour les sciences humaines et sociales.

③ « Il est interdit d'exploiter la mise à disposition permise au titre du premier alinéa dans le cadre d'une activité d'édition à caractère commercial.

④ « II. – Dès lors que les données issues d'une activité de recherche, financée au moins pour moitié par des dotations de l'État, des collectivités territoriales, des établissements publics, des subventions d'agences de financement nationales ou par des fonds de l'Union européenne, ne sont pas protégées par un droit spécifique, ou une réglementation particulière, et qu'elles ont été rendues publiques par le chercheur, l'établissement ou l'organisme de recherche, leur réutilisation est libre.

⑤ « III. – L'éditeur d'un écrit scientifique mentionné au I ne peut limiter la réutilisation des données de la recherche rendues publiques dans le cadre de sa publication.

⑥ « IV. – Les dispositions du présent article sont d'ordre public et toute clause contraire à celles-ci est réputée non écrite. »

Article 18

① I. – Il est ajouté à l'article 22 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés un I *bis* ainsi rédigé :

② « I *bis*. – Par dérogation aux 1° du I et du II de l'article 27, font également l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés les traitements qui portent sur des données personnelles parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, ou qui requièrent une consultation de ce répertoire, lorsque ces traitements ont exclusivement des finalités de statistique publique, et ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9, à la condition que le numéro d'inscription à ce répertoire ait préalablement fait l'objet d'une opération cryptographique lui substituant un code statistique non signifiant afin de circonscrire le traitement des données concernées au sein du seul service statistique public.

③ « Un décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale informatique et libertés, définit les modalités d'application du précédent alinéa. »

④ II. – Au I de l'article 25, il est ajouté un 9° ainsi rédigé :

⑤ « 9° Par dérogation aux 1° du I et du II de l'article 27, les traitements qui portent sur des données personnelles parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, ou qui requièrent une consultation de ce répertoire, lorsque ces traitements ont exclusivement des finalités de recherche scientifique ou historique, ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9, à la condition que le numéro d'inscription à ce répertoire ait préalablement fait l'objet d'une opération cryptographique lui substituant un code spécifique non signifiant, propre à chaque projet de recherche, afin de ne pas permettre son utilisation en dehors du projet de recherche. L'opération cryptographique, et, le cas échéant, l'interconnexion de deux fichiers par l'utilisation du code spécifique non signifiant qui en est issu, sont assurés par une personne distincte de la personne responsable du traitement.

⑥ « Un décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale informatique et libertés, définit les modalités d'application du précédent alinéa. »

⑦ III. – Aux 1° des I et II de l'article 27, avant les mots : « les traitements » sont ajoutés les mots : « Sous réserve du I *bis* de l'article 22 et du 9° du I de l'article 25, ».

TITRE II

LA PROTECTION DES DROITS DANS LA SOCIÉTÉ NUMÉRIQUE

CHAPITRE I^ER

Environnement ouvert

Section 1

Neutralité de l'internet

Article 19

① I. – Au II de l'article L. 32-1 du code des postes et des communications électroniques, après le 5°, il est inséré un alinéa ainsi rédigé :

② « *5° bis* La neutralité de l'internet, définie au *p* du I de l'article L. 33-1. »

③ II. – Au 2° de l'article L. 32-4 du même code, après les mots : « les conditions techniques et tarifaires d'acheminement du trafic » sont ajoutés les mots : « , y compris de gestion, » et la phrase est complétée par les mots : « , notamment en vue d'assurer le respect de la neutralité de l'internet mentionnée au *p* du I de l'article L. 33-1 ».

④ III. – Le I de l'article L. 33-1 du même code est ainsi modifié :

⑤ 1° Après le *o*, il est inséré un alinéa ainsi rédigé :

⑥ « *p)* La neutralité de l'internet, qui consiste à garantir l'accès à l'internet ouvert régi par le règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures

relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union. » ;

⑦ 2° Au dernier alinéa, les mots : « *a* à *o* » sont remplacés par les mots : « *a* à *p* ».

⑧ IV. – Au 3° de l'article L. 36-7 du même code, après les mots : « à l'intérieur de l'Union » sont insérés les mots : « , du règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union ».

⑨ V. – Le 5° du II de l'article L. 36-8 du même code est ainsi modifié :

⑩ 1° Après les mots : « d'acheminement » sont insérés les mots : « , y compris de gestion, » ;

⑪ 2° La phrase est complétée par les mots : « , en vue notamment d'assurer le respect de la neutralité de l'internet mentionnée au *p* du I de l'article L. 33-1 ».

⑫ VI. – L'article L. 36-11 du même code est ainsi modifié :

⑬ 1° Au premier alinéa, après les mots : « des fournisseurs de services de communications électroniques », sont insérés les mots : « ou des personnes fournissant des services de communication au public en ligne » ;

⑭ 2° Au premier alinéa du I, le mot : « ou » est remplacé par le mot : « , par » et après les mots : « fournisseur de services de communications électroniques » sont insérés les mots : « , ou par une personne fournissant des services de communication au public en ligne » ;

⑮ 3° Après le troisième alinéa du I, il est inséré un alinéa ainsi rédigé :

⑯ « – aux dispositions du règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et

services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union. » ;

⑰ 4° Après le sixième alinéa du I, il est inséré un alinéa ainsi rédigé :

⑱ « Lorsque l'Autorité estime qu'il existe un risque caractérisé qu'un exploitant de réseau ou une personne fournissant des services de communications électroniques ne respecte pas ses obligations, résultant des dispositions et prescriptions mentionnées au I, à l'échéance prévue initialement, elle peut mettre en demeure l'exploitant ou le fournisseur de s'y conformer à cette échéance. » ;

⑲ 5° Au premier alinéa du II, les mots : « ou un fournisseur de services de communications électroniques » sont remplacés par les mots : « , un fournisseur de services de communications électroniques ou un fournisseur de services de communication au public en ligne ».

Article 20

① L'article L. 33-1 du même code est complété par un VI ainsi rédigé :

② « VI. – Aucune limitation technique ou contractuelle ne peut être apportée à un service d'accès à l'internet, qui aurait pour objet ou effet d'interdire à un utilisateur de ce service qui en fait la demande :

③ « 1° D'accéder, depuis un point d'accès à l'internet, à des données enregistrées sur un équipement connecté à l'internet, via le service d'accès auquel il a souscrit ;

④ « 2° Ou de donner à des tiers accès à ces données. »

Section 2

Portabilité et récupération des données

Article 21

① I. – Le code de la consommation est ainsi modifié :

② 1° Au chapitre I^{er} du titre II du livre I^{er}, il est inséré une section 20 ainsi rédigée :

③ *« Section 20*

④ ***« Récupération et portabilité de données***

⑤ « *Art. L. 121-120.* – Le consommateur dispose en toutes circonstances d'un droit de récupération de données dans les conditions prévues à la présente section.

⑥ *« Sous-section 1*

⑦ *« Services de courrier électronique*

⑧ « *Art. L. 121-121.* – Tout fournisseur d'un service de courrier électronique qui comprend la mise à disposition d'une adresse de courrier électronique doit proposer une fonctionnalité gratuite permettant au consommateur de transférer directement les messages qu'il a émis ou reçus au moyen de ce service et qui sont conservés par un système de traitement automatisé mis en œuvre ce fournisseur, ainsi que sa liste de contacts, vers un autre fournisseur de service de courrier électronique comprenant la mise à disposition d'une adresse de courrier électronique, dans la limite de la capacité de stockage de ce nouveau service.

⑨ « À cette fin, il ne peut refuser de fournir à cet autre fournisseur les informations nécessaires à la mise en place des fonctionnalités mentionnées au premier alinéa, notamment celles relatives à leurs règles techniques et aux standards applicables.

⑩ « Ce fournisseur informe le consommateur de manière loyale, claire et transparente du droit mentionné au premier alinéa.

⑪ « Il est tenu de proposer gratuitement au consommateur, lorsque celui-ci change de fournisseur, une offre lui permettant de continuer, pour une durée de six mois à compter de la résiliation ou de la désactivation du service, à avoir accès gratuitement au courrier électronique reçu sur l'adresse électronique initialement attribuée.

⑫ *« Sous-section 2*

⑬ *« Récupération des données stockées en ligne*

⑭ « *Art. L. 121-122.* – Tout fournisseur d'un service de communication au public en ligne propose, en prenant toutes les mesures nécessaires à cette fin, notamment en termes d'interface de programmation, au consommateur une fonctionnalité gratuite permettant la récupération licite :

⑮ « 1° De tous les fichiers mis en ligne par le consommateur ;

⑯ « 2° De toutes les données associées au compte utilisateur du consommateur et résultant de l'utilisation de ce compte, notamment les données relatives au classement de contenus, dans un standard ouvert et aisément réutilisable, lisible par une machine et pouvant être exploité par un système de traitement automatisé.

⑰ « La fonctionnalité prévue au premier alinéa offre au consommateur une faculté de requête unique étendue au moins à un type ou un format de fichiers ou données.

⑱ « Pour les données résultant d'un traitement de données collectées auprès d'un consommateur et qui ne peuvent pas être récupérées dans un standard ouvert et aisément réutilisable, le fournisseur de service de communication au public en ligne informe clairement le consommateur, avant la conclusion d'un contrat et dans le contrat, de l'impossibilité ou de la possibilité de récupérer ces données et, le cas échéant, des modalités de cette récupération et de la forme, notamment le format de fichier, sous laquelle ces données sont récupérables. Le fournisseur de service de communication au public en ligne précise le cas échéant le caractère ouvert et interopérable du format de fichier utilisé.

⑲ *« Sous-section 3*

⑳ *« Champ d'application et sanctions*

㉑ « *Art. L. 121-123.* – La présente section est également applicable aux services fournis aux professionnels pour l'exercice de leurs activités à titre principal ou accessoire.

㉒ « *Art. L. 121-124.* – Tout manquement aux articles L. 121-121 et L. 121-122 est passible d'une amende administrative dont le montant ne peut excéder 3 000 € pour une personne physique et 15 000 € pour une personne morale. L'amende est prononcée dans les conditions prévues à l'article L. 141-1-2.

㉓ « *Art. L. 121-125.* – La présente section ne s'applique pas aux fournisseurs d'un service de communication au public en ligne dont le nombre de comptes utilisateurs ayant fait l'objet d'une connexion au cours des douze derniers mois est inférieur à un seuil fixé par décret. » ;

㉔ 2° Au 2° du I de l'article L. 141-1, les mots : « 12 et 15 » sont remplacés par les mots : « 12, 15 et 20 ».

㉕ II. – Les dispositions du présent article entrent en vigueur dix-huit mois à compter de la date de publication de la présente loi.

Section 3

Loyauté des plateformes

Article 22

① L'article L. 111-5-1 du même code est ainsi modifié :

② 1° Le premier alinéa est remplacé par les dispositions suivantes :

③ « Est qualifié d'opérateur de plateforme en ligne, toute personne exerçant à titre professionnel des activités consistant à classer ou référencer des contenus, biens ou services proposés ou mis en ligne par des tiers, ou à mettre en relation, par voie électronique, plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service, y compris à titre non rémunéré, ou de l'échange ou du partage d'un bien ou d'un service.

④ « Sans préjudice des obligations prévues à l'article 19 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente sur les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, biens ou services auxquels ce service permet d'accéder. Il fait notamment apparaître clairement l'existence ou non d'une relation contractuelle ou de liens capitalistiques avec les personnes référencées, l'existence ou non d'une rémunération par les lesdites personnes et, le cas échéant, l'impact de celle-ci sur le classement des contenus, biens ou services proposés. » ;

⑤ 2° Aux deuxième et troisième alinéas qui deviennent les troisième et quatrième alinéas, les mots : « la personne mentionnée au premier alinéa du présent article est également tenue » sont remplacés par les mots : « l'opérateur de la plateforme en ligne est également tenu ».

Article 23

① Après l'article L. 111-5-1 du même code, il est inséré un article L. 111-5-2 ainsi rédigé :

② « *Art. L. 111-5-2.* – I. – Les opérateurs de plateformes en ligne, dont l'activité dépasse un seuil de nombre de connexions défini par décret :

③ « 1° Élaborent et diffusent auprès des consommateurs des bonnes pratiques visant à renforcer leurs obligations de clarté, de transparence et de loyauté ;

④ « 2° Définissent des indicateurs permettant d'apprécier le respect de leurs obligations de clarté, de transparence et de loyauté ;

⑤ « 3° Rendent périodiquement publics les résultats de l'évaluation des indicateurs mentionnés au 2°.

⑥ « Les informations mentionnées aux 1° à 3° sont communiquées à l'autorité administrative compétente.

⑦ « II. – L'autorité administrative compétente peut notamment :

⑧ « 1° Procéder à des enquêtes dans les conditions prévues au premier alinéa du II de l'article L. 141-1, en particulier auprès des opérateurs de plateformes et de tout organisme participant à l'évaluation de leurs pratiques ;

⑨ « 2° Publier la liste des plateformes en ligne ne respectant pas leurs obligations au titre de l'article L. 115-5-1 ;

⑩ « 3° Recueillir auprès des opérateurs de plateformes en ligne mentionnés au I les données nécessaires en vue de la publication par leurs soins, ou par un organisme désigné à cet effet, des résultats de ces indicateurs, lorsqu'elle estime que les informations mises à la disposition des consommateurs ne permettent pas au consommateur d'apprécier et de comparer les pratiques mises en œuvre.

⑪ « Un décret précise les modalités d'application du présent II. »

Article 24

① Le chapitre I^er^ du titre I^er^ du livre I^er^ du même code est ainsi modifié :

② 1° Après l'article L. 111-5-2, il est inséré un article L. 111-5-3 ainsi rédigé :

③ « *Art. L. 111-5-3.* – Sans préjudice des obligations d'information prévues à l'article 19 de la loi n° 2004-575 du 21 juin 2004 pour la

confiance dans l'économie numérique et aux articles L. 111-5-1 et L. 111-5-2, toute personne physique ou morale dont l'activité consiste, à titre principal ou accessoire, à collecter, modérer ou diffuser des avis en ligne provenant de consommateurs, est tenue de délivrer à ces consommateurs une information loyale, claire et transparente sur les modalités de vérification des avis mis en ligne.

④ « Elle leur précise si les avis qu'elle a mis en ligne font l'objet ou non d'une vérification et, si tel est le cas, elle leur indique les caractéristiques principales de la vérification mise en œuvre.

⑤ « Les modalités et le contenu de ces informations sont fixés par décret. » ;

⑥ 2° À l'article L. 111-6-1 du même code, les mots : « et L. 111-5-1 » sont remplacés par les mots : « , L. 111-5-1 et L. 111-5-3 ».

Article 25

① I. – L'article L. 121-83 du même code est ainsi modifié :

② 1° Après le *b*, il est inséré un *b* bis ainsi rédigé :

③ « *b* bis*)* Une explication claire et compréhensible en ce qui concerne les débits minimums normalement disponibles, maximums montants et descendants fournis et annoncés, lorsqu'il s'agit de services d'accès à internet fixe, et en ce qui concerne les débits maximums montants et descendants estimés et annoncés, dans le cadre de services d'accès à internet mobile, ainsi que l'incidence d'un écart significatif par rapport au débit prévu au contrat sur la disponibilité des services offerts. » ;

④ 2° Le *g* est complété par les mots : « , de protection de la vie privée et des données à caractère personnel, ainsi que l'impact des limitations de volume, de débits ou d'autres paramètres sur la qualité de l'accès à internet, en particulier l'utilisation de contenus, d'applications et de services, y compris ceux bénéficiant d'une qualité optimisée. »

⑤ II. – L'article L. 121-83 du même code dans sa rédaction issue de la présente loi est applicable aux contrats conclus ou reconduits postérieurement à la promulgation de cette même loi.

CHAPITRE II

Protection de la vie privée en ligne

Section 1

Protection des données à caractère personnel

Article 26

① Au chapitre II de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, il est ajouté un article 5 *bis* ainsi rédigé :

② « *Art. 5* bis. – Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »

Article 27

① Après le 7° de l'article 32 de la même loi, il est ajouté un 8° ainsi rédigé :

② « 8° De la durée de conservation des catégories de données traitées. »

Article 28

① I. – Après l'article 43 de la même loi, il est inséré un article 43-1 ainsi rédigé :

② « *Art. 43-1.* – Sauf dans le cas prévu par le 1° du I de l'article 26, lorsque le responsable de traitement dispose d'un site Internet, il permet à toute personne d'exercer par voie électronique les droits prévus par le présent chapitre.

③ « Lorsque le responsable du traitement est une autorité administrative au sens du I de l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, le principe énoncé à l'alinéa précédent est mis en œuvre dans les conditions fixées par cette ordonnance. »

④ II. – Il est ajouté à l'article 4 de l'ordonnance du 8 décembre 2005 précitée un alinéa ainsi rédigé :

⑤ « Les dispositions de l'alinéa précédent s'appliquent lorsque, en vertu de l'article 43-1 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, au fichiers et aux libertés, l'autorité administrative doit permettre à toute personne d'exercer par voie électronique les droits prévus au chapitre V de cette loi. »

Article 29

① Le 4° de l'article 11 de la même loi est ainsi modifié :

② 1° Au troisième alinéa, sont ajoutés à la première phrase les mots : « ou sur les dispositions de tout projet de loi ou de décret relatives à la protection des données à caractère personnel ou au traitement de telles données. » ;

③ 2° Il est ajouté un sixième et un septième alinéas ainsi rédigés :

④ « *e)* Elle conduit une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques, en impliquant des personnalités qualifiées et en organisant des débats publics ;

⑤ « *f)* Elle promeut, dans le cadre de ses missions, l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données. »

Article 30

① Il est inséré dans la même loi un article 37-1 ainsi rédigé :

② « *Art. 37-1.* – La Commission nationale de l'informatique et des libertés peut certifier la conformité à la présente loi de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques mises en ligne dans les conditions prévues par le chapitre II du titre I^{er} de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

③ « Il en est tenu compte, le cas échéant, pour la mise en œuvre des sanctions prévues au chapitre VII. »

Article 31

① À la fin de l'article 36 de la même loi, il est ajouté un alinéa ainsi rédigé :

② « – soit en vertu de directives de la personne concernée, dans les conditions définies au II de l'article 40. »

Article 32

① L'article 40 de la même loi est ainsi modifié :

② 1° Le premier alinéa est précédé d'un I ;

③ 2° Après le cinquième alinéa, sont ajoutées les dispositions suivantes :

④ « II. – Sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte.

⑤ « En cas de non-exécution de l'effacement des données personnelles ou d'absence de réponse du responsable de traitement dans un délai d'un mois après la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur la demande dans un délai de quinze jours à compter de la date de réception de la réclamation.

⑥ « Les dispositions des deux alinéas précédents ne s'appliquent pas lorsque le traitement de données à caractère personnel est nécessaire :

⑦ « 1° Pour exercer le droit à la liberté d'expression et d'information ;

⑧ « 2° Pour respecter une obligation légale qui requiert le traitement des données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

⑨ « 3° Pour des motifs d'intérêt public dans le domaine de la santé publique ;

⑩ « 4° À des fins d'archivage dans l'intérêt public ou à des fins scientifiques statistiques et historiques ;

⑪ « 5° À la constatation, à l'exercice ou à la défense de droits en justice.

⑫ « Les modalités d'application du présent II sont fixées par décret en Conseil d'État. » ;

⑬ 3° Les deux derniers alinéas sont supprimés ;

⑭ 4° Sont ajoutées à la fin de l'article les dispositions suivantes :

⑮ « II. – Toute personne peut définir des directives relatives à la conservation et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières.

⑯ « Les directives générales concernent l'ensemble des données à caractère personnel de leur auteur et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés.

⑰ « Les directives particulières concernent les traitements de données à caractère personnel qu'elles désignent. Elles sont enregistrées auprès des responsables de traitement concernés.

⑱ « Les directives définissent la manière dont la personne entend que soient exercés après son décès les droits qu'elle détient en application de la présente loi. Ces directives sont sans préjudice des dispositions applicables aux données à caractère personnel relevant du régime sur les archives publiques.

⑲ « Lorsque les directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette communication doit être effectuée dans le respect de la présente loi.

⑳ « La personne peut modifier ou révoquer ses directives à tout moment.

㉑ « Les directives mentionnées au premier alinéa du présent II peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. À défaut de désignation, ont cette qualité dans l'ordre suivant : les descendants, le conjoint contre lequel n'existe pas un jugement passé en force de chose jugée de séparation de corps ou qui n'a pas contracté un nouveau mariage, les héritiers autres que les descendants qui recueillent

tout ou partie de la succession et les légataires universels ou donataires de l'universalité des biens à venir.

㉒ « Sauf lorsque la personne concernée a exprimé une volonté contraire dans les directives mentionnées au premier alinéa du présent II, ou en l'absence de directives, ses héritiers, dans l'ordre mentionné au précédent alinéa, peuvent exercer après son décès les droits mentionnés à la présente section.

㉓ « Tout prestataire d'un service de communication au public en ligne informe l'utilisateur du sort des données qui la concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne. »

Article 33

① I. – L'article 45 de la même loi est ainsi modifié :

② 1° Le I est remplacé par les dispositions suivantes :

③ « I. – Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à 24 heures.

④ « Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la Commission prononce la clôture de la procédure.

⑤ « Dans le cas contraire, la formation restreinte de la Commission peut prononcer, après une procédure contradictoire, les sanctions suivantes :

⑥ « 1° Un avertissement ;

⑦ « 2° Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'État ;

⑧ « 3° Une injonction de cesser le traitement, lorsque celui-ci relève des dispositions de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.

⑨ « Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer, sans mise en demeure préalable, l'une des sanctions prévues au I du présent article. » ;

⑩ 2° Au III, les mots : « de sécurité » sont supprimés.

⑪ II. – Après la première phrase du deuxième alinéa de l'article 46 de la loi du 6 janvier 1978 précitée, il est inséré une phrase ainsi rédigée : « Elle peut ordonner que les personnes sanctionnées informent individuellement de cette sanction, à leur frais, chacune des personnes concernées. »

Section 2

Confidentialité des correspondances privées

Article 34

① L'article L. 32-3 du code des postes et des communications électroniques est remplacé par les dispositions suivantes :

② « *Art. L. 32-3.* – I. – Les opérateurs, ainsi que les membres de leur personnel, sont tenus de respecter le secret des correspondances. Le secret couvre le contenu de la correspondance, l'identité des correspondants ainsi que, le cas échéant, l'intitulé du message et les documents joints à la correspondance.

③ « II. – Les éditeurs de services de communication au public en ligne permettant aux utilisateurs de ces services d'échanger des correspondances, ainsi que les membres de leur personnel, sont tenus de respecter le secret de celles-ci. Le secret couvre le contenu de la correspondance, l'identité des correspondants ainsi que, le cas échéant, l'intitulé du message et les documents joints à la correspondance.

④ « Tout traitement automatisé d'analyse du contenu de la correspondance en ligne, de l'intitulé ou des documents mentionnés à l'alinéa précédent constitue une atteinte au secret des correspondances, sauf lorsque ce traitement a pour fonction l'affichage, le tri ou l'acheminement de ces correspondances, la fourniture d'un service bénéficiant uniquement à l'utilisateur ou la détection de contenus non sollicités ou de programmes informatiques malveillants.

⑤ « III. – Les opérateurs et les éditeurs mentionnés aux I et II sont tenus de porter à la connaissance de leur personnel les obligations résultant de ces dispositions.

TITRE III

L'ACCÈS AU NUMÉRIQUE

CHAPITRE I^ER

Numérique et territoires

Section 1

Compétences et organisation

Article 35

① Le chapitre V du titre II du livre IV du code général des collectivités territoriales est complété par un article L. 1425-3 ainsi rédigé :

② « *Art. L. 1425-3.* – Dans les domaines de compétence que la loi leur attribue, les conseils départementaux ou les conseils régionaux peuvent établir une stratégie de développement des usages et services numériques, identifier les zones qu'ils desservent et présenter une stratégie de développement de ceux-ci, sur leur territoire. Cette stratégie, qui a une valeur indicative, vise à favoriser la cohérence des initiatives publiques et leur bonne articulation avec l'investissement privé, ainsi que la mise en place de ressources partagées et mutualisées, y compris en matière de médiation numérique, afin de doter l'ensemble des territoires d'un maillage équilibré de services numériques. Elle permet en particulier d'assurer l'existence, sur l'ensemble du territoire concerné, d'une offre de services de médiation numérique de nature à répondre aux besoins identifiés d'accompagnement de la population à l'utilisation des services et technologies numériques. Elle constitue un volet du schéma directeur territorial d'aménagement numérique. Le projet de stratégie peut faire l'objet d'une concertation pour recueillir les observations du public. »

Article 36

① I. - Après le deuxième alinéa du I de l'article L. 1425-1 du code général des collectivités territoriales, il est ajouté un alinéa ainsi rédigé :

ANNEXE N°4

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PROJET DE LOI

pour une République numérique

NOR : EINI1524250L/Bleue

ETUDE D'IMPACT

9 décembre 2015

TITRE I^er

La circulation des données et du savoir

Chapitre I^er

Economie de la donnée

Section 1
Ouverture de l'accès aux données publiques

Article 1^er
Communication de données entre administrations publiques

1. **État des lieux**

Bien que l'article L. 311-1 du code des relations entre le public et l'administration prévoie que les administrations sont tenues de communiquer les documents administratifs qu'elles détiennent aux personnes qui en font la demande, la CADA a toujours considéré que ce droit « d'accès citoyen » n'était pas ouvert aux personnes publiques.

Le 13 septembre 2012, la CADA a confirmé sa doctrine selon laquelle le droit d'accès instauré par la loi du 17 juillet 1978, à l'inverse de celui régissant les informations environnementales sur le fondement des articles L. 124-1 et suivants du code de l'environnement transposant la directive 2003/4/CE du 28 janvier 2003, n'a pas en l'état du droit vocation à inclure la transmission d'informations entre autorités administratives et qu'il ne lui appartenait d'arbitrer, même de façon consultative, des différends entre autorités administratives.

La CADA a identifié ce point et y a consacré un paragraphe dans son rapport d'activité au titre de l'année 2012. Elle a ainsi recommandé une modification de la loi en ce sens.

Cette interprétation, tirée de la rédaction actuelle de l'article L. 311-1 du code des relations entre le public et l'administration, conduit à traiter de manière plus défavorable les demandes de communication émanant des administrations que celles exprimées par des particuliers.

Cette interprétation n'empêche pas, en elle-même, la communication de données entre les administrations, mais elle ne permet pas de disposer d'un cadre législatif harmonisé relatif à cette communication, ce qui peut prêter à des divergences de pratiques entre les administrations.

En particulier, en l'absence de précision dans la loi d'un cadre législatif relatif à ces échanges, certaines administrations ont pu considérer qu'aucun droit de communication n'existait au profit d'autres administrations, ou que ce droit de communication devait être considéré comme une réutilisation de données publiques, pouvant ouvrir droit à tarification, au sens du chapitre II du titre Ier de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures

d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

Enfin, l'imprécision sur le cadre législatif de la communication des données entre les administrations induit souvent une négociation et la signature d'une convention entre l'administration productrice et l'administration utilisatrice sur le cadre juridique, les conditions de transmission, d'usage, voire de tarification des données transmises, qui constituent des coûts administratifs inutiles et une perte de temps.

2. Objectifs poursuivis

Le présent projet de loi vise à donner aux administrations l'accès aux informations publiques d'autres administrations tout en permettant leur utilisation à des fins de service public autres que celles pour lesquelles elles ont été élaborées.

Le projet d'article vise à renforcer la communication des données entre les administrations et à donner un cadre législatif à ces échanges. Cet article a ainsi pour but de favoriser l'échange d'informations nécessaire au bon fonctionnement des administrations, échange qui participe de la modernisation de l'action publique et contribue à améliorer la prise de décision au sein des administrations.

Il a en effet pu être identifié l'existence de nombreux freins à la bonne circulation des données entre les administrations, ces freins pouvant être budgétaires, sociologiques ou juridiques.

Ces freins entrainent des conséquences sous-optimales en termes de qualité, d'efficience, de réactivité de l'action publique, mais peuvent également susciter des effets de renoncement à la donnée (par méconnaissance ou par abandon face à la complexité d'accès ou le refus opposé par l'administration productrice), ou des stratégies de contournement (par exemple par constitution de bases de données équivalentes à celles produites par une autre administration).

De plus, l'introduction dans la loi d'une obligation de transmission des données entre administrations permettrait de réduire les coûts administratifs liés à la négociation des conditions de transmission des données entre les administrations, en supprimant le temps passé par les administrations à expertiser la possibilité juridique de transmettre des données publiques à une autre administration.

En outre, ce projet d'article participe de l'amélioration de la circulation des données entre les administrations. Il est de nature à engendrer plusieurs externalités positives, notamment des externalités de production, des externalités de consommation et des externalités technologiques. En posant un principe d'obligation de communication entre les administrations, il ne peut que développer les effets de réseau entre les administrations permettant un meilleur usage coordonné des données produites par les administrations, un renforcement de la transparence de l'action publique par ce fait, le développement de projets communs, permettant de réaliser des gains de productivité budgétaire et socioéconomiques.

Enfin, ces nouvelles dispositions mettront fin aux situations parfois aberrantes où la personne qui demande l'accès à un document administratif se voit traitée différemment selon qu'elle se présente à titre personnel ou en tant que représentant d'une autorité administrative.

Cette mesure s'inscrit dans la continuité de la loi n° 2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit et la loi n° 2012-387 du 22 mars 2012 relative à la simplification du droit et à l'allégement des démarches administratives, et des évolutions récentes liées à l'ordonnance n° 2015-507 du 7 mai 2015 relative à l'adaptation du secret professionnel dans les échanges d'informations entre autorités administratives et à la suppression de la production de pièces justificatives. Dans ce contexte, l'article 16A de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, codifié depuis à l'article L. 114-8 du code des relations entre le public et l'administration, prévoit que les autorités administratives doivent désormais échanger entre elles toutes informations ou données nécessaires pour traiter les demandes présentées par un usager ou les déclarations transmises par celui-ci en application d'un texte législatif ou réglementaire.

Cependant, le présent projet d'article ne se limite pas aux situations dans lesquelles il s'agit d'une nécessité pour traiter la demande d'un usager.

Etant donné le caractère sensible ou confidentiel de certaines informations, cette obligation d'échange s'applique sous réserve des dispositions des articles L. 311-5 et L. 311-6, qui excluent la communication de certains documents, ou qui la réduisent, et en conformité avec l'article L. 114-8 du code des relations entre le public et l'administration. De même, ce principe est sans incidence sur le régime juridique des données couvertes par un secret protégé par la loi qui disposent de conditions particulières d'accès.

3. Analyse des impacts des dispositions envisagées

Le rapport d'Adnène Trojette sur l'ouverture des données publiques[1] a très largement démontré que les administrations sont parmi les principaux réutilisateurs des données publiques. Ce nouveau dispositif bénéficie au fonctionnement interne de l'État, des collectivités, des organismes de protection sociale et de leurs établissements publics en ce qu'elle contribue à faciliter la circulation entre les administrations de données, produites en premier lieu dans le cadre d'une mission de service public. La circulation des données au sein des administrations est une condition essentielle de l'efficacité de leur mission, et le préalable à leur exploitation via de nouvelles approches de type sciences de données (datasciences).

Ces dispositions pourraient produire, à court terme, de nombreux effets favorables en termes de qualité et de précision des politiques publiques au moins à trois niveaux : lors de l'élaboration des évaluations préalables de ces politiques ; lors de la mise en œuvre de ces politiques par la constitution d'outils d'aides à la décision fondés sur l'exploitation des données ; lors de l'évaluation *ex post* de ces politiques publiques.

Un meilleur accès aux données du service hydrographique et océanographique de la marine renforcerait par exemple la qualité des actions de l'État et de plusieurs opérateurs de l'État en matière de protection des milieux marins et littoraux, de biodiversité et de contrôle des pêches.

[1] M. Adnène Trojette sur l' « Ouverture des données publiques, les exceptions au principe de gratuité sont-elles toutes légitimes ? » remis au Premier ministre le 15 juillet 2013

Impact sur les collectivités territoriales

Ces dispositions faciliteront notamment les demandes d'informations publiques adressées par les collectivités territoriales aux services de l'État et les demandes d'informations publiques adressées par les services de l'État aux collectivités territoriales.

Sans pouvoir augurer avec précision du nombre de demandes de communication qui émaneraient des administrations suite à la mise en œuvre du nouveau dispositif, il ressort de la base des avis de la CADA, que la commission a eu à traiter, sur la période 2012-2015, une dizaine de demandes de droit d'accès émanant d'autorités administratives. Il apparait donc que le nombre de dossiers traités est modeste, ce qui s'explique par l'absence de cadre législatif relatif à ces échanges. Il ressort également de l'examen des dossiers traités par la commission, que les collectivités territoriales sont dans la grande majorité des cas à l'initiative de ces demandes de communication.

Ainsi, les collectivités territoriales seraient les principales bénéficiaires du nouveau dispositif qui facilitera notamment les demandes de communication d'informations publiques adressées aux services de l'État. Dans ces conditions, l'impact apparait plutôt favorable aux collectivités sans que l'on puisse identifier, à ce stade, de charges trop contraignantes sur celles-ci.

A titre d'exemple, la communication des données du Registre Parcellaire Graphique a pu être demandée par les syndicats intercommunaux chargés d'améliorer les pratiques agricoles afin de diminuer les pollutions d'origine agricole, répondant à un enjeu environnemental majeur. L'accès des collectivités territoriales au répertoire national des associations (RNA) du ministère de l'intérieur, créé par l'arrêté du 24 octobre 2009 dans la démarche de simplification des procédures administratives, pourrait également être ainsi facilité. Un accès élargi à ce registre contenant plus de deux millions d'associations permettrait dès lors une meilleure allocation des ressources pour les collectivités territoriales qui interviennent dans le financement des associations, et une meilleure connaissance du tissu associatif sur leur territoire.

4. Consultations menées

Le Conseil national d'évaluation des normes et la Commission d'accès aux documents administratifs ont été consultés.

5. Outre-mer

L'article 46 du projet de loi rend l'article 1er applicable en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

Article 2
Communication des décisions
prises sur le fondement d'un traitement algorithmique

1. État des lieux

La transformation numérique de l'administration et la profusion des données rendent de plus en plus fréquents les recours aux programmes informatiques et aux traitements algorithmiques, qui outillent le travail des agents publics et préparent les décisions des administrations. De nombreux systèmes, fondés sur des traitements algorithmiques, aboutissent à des résultats ou à des outils d'aide à la décision qui impactent la vie des individus.

Si l'article 10 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit qu'« *aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* », et si le 5° de l'article 39 de cette même loi donne à toute personne physique justifiant de son identité le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir, sous réserve de ne pas porter atteinte au droit d'auteur, les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé, ces dispositions ne permettent pas de garantir une complète information du citoyen.

En effet, de nombreux programmes utilisant des traitements algorithmiques traitent des données qui ne sont pas toujours à caractère personnel, et qui – sans constituer l'unique fondement d'une décision – fournissent des éléments sur lesquels s'appuie la restitution finale des résultats du traitement.

Par ailleurs, les décisions individuelles faisant intervenir des traitements algorithmiques peuvent concerner aussi des personnes morales, lesquelles ne bénéficient pas des dispositions de la loi du 6 janvier 1978.

Ainsi, les seules dispositions de l'article 39 de la loi du 6 janvier 1978, par leur champ, portée et limites, qui sont exposés dans le tableau ci-dessous, ne permettent pas d'assurer une information complète des personnes soumises à des traitements algorithmiques.

Art. 39 de la loi du 6 janvier 1978	Art. 2 du présent projet de loi
Personnes physiques	Toute personne, physique ou morale
Traitements automatisé s'inscrivant dans le cadre d'un traitement de données à caractère personnel	Tout traitement algorithmique fondement d'une décision individuelle

Informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé	Règles définissant le traitement algorithmique ainsi que les principales caractéristiques de sa mise en œuvre

Le projet d'article vient ainsi utilement compléter le cadre juridique de la loi du 6 janvier 1978.

2. Objectifs poursuivis

Le présent article vise à renforcer la transparence de l'action publique, en ajoutant une possibilité nouvelle pour les citoyens et les personnes morales de comprendre les fondements algorithmiques de décisions qui les concernent. Ainsi, le citoyen qui fait l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique, que ce traitement s'inscrive dans le cadre d'une traitement de données à caractère personnel ou non, aura le droit d'interroger l'administration afin de connaitre les règles gouvernant le traitement algorithmique ainsi que les caractéristiques principales de sa mise en œuvre (quel est le fonctionnement du traitement, quelles règles et bases de calcul ont été utilisées, quels paramètres ont été mis en œuvre...)

A titre d'exemple, le système Admission Post Bac (APB) permet d'affecter les étudiants dans des filières d'enseignement supérieur. Le recours à ce logiciel, reposant sur des traitements algorithmiques, peut susciter des interrogations sur les mécaniques et les règles de fonctionnement qui conduisent à un résultat décisif pour l'avenir des étudiants : comment ce système est-il paramétré ? Quelle est la part de tirage au sort dans la procédure d'affectation pour les filières les plus demandées ? Comment s'assurer qu'il n'est pas possible de « tricher » avec le système ?

Les dispositions combinées du projet de loi et de l'article 39 de la loi du 6 janvier 1978 permettront aux personnes tant physiques que morales, d'avoir une information complète sur les règles mises en œuvre dans le cadre d'un traitement algorithmique, les principales caractéristiques de celui-ci : la loi leur permettra ainsi, de façon effective, de connaître et, le cas échéant, de contester la logique algorithmique présidant à la prise de décision.

3. Analyse des impacts des dispositions envisagées

Si un citoyen en fait la demande, l'administration devra donc être en mesure de communiquer les caractéristiques du traitement, notamment les objectifs, les finalités et les contraintes du système, et communiquer à l'individu concerné par la décision un exposé des paramètres, principales caractéristiques et des règles générales de l'algorithme, ainsi que celles qui lui ont été appliquées particulièrement.

Impact sur les collectivités territoriales

Ces dispositions s'appliqueront similairement aux collectivités territoriales.

4. Consultations menées

Le Conseil national d'évaluation des normes et la Commission d'accès aux documents administratifs ont été consultés.

5. Textes d'application et Outre-mer

Il est prévu un décret en Conseil d'État qui fixera les conditions d'application du présent article, afin de vérifier que le dispositif mis en place comporte toutes les garanties nécessaires en matière notamment de respect des secrets protégés par la loi.

L'article 46 du projet de loi rend le présent article applicable en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises. L'article 43 modifie, en conséquence, les articles L. 552-8, L. 553-2, L. 562-8, L. 563-2, L. 574-1, L. 574-5 du code des relations entre le public et l'administration.

Articles 3, 4 et 5
Elargissement du champ de diffusion par l'administration

1. État des lieux

1.1 Eléments juridiques

La loi du 17 juillet 1978, codifiée dans le code des relations entre le public et l'administration, prévoit deux régimes d'accès aux documents administratifs : la communication et la diffusion publique. Cependant, elle ne prévoit pas l'obligation pour les administrations et personnes privées chargées d'une mission de service public de diffuser publiquement les documents qui sont librement communicables. En effet, l'alinéa 1er de l'article L. 312-2 du code précité prévoit une diffusion obligatoire seulement pour certains documents déterminés comportant une interprétation du droit positif, telles que les directives, instructions, circulaires. L'article L. 321-1, quant à lui, prévoit une simple possibilité de diffusion des autres documents administratifs.

1.2 État d'avancement de la politique française d'open data

Le Gouvernement s'est engagé dans une politique ambitieuse d'ouverture et de partage des données publiques (« Open Data »). Cette priorité a été inscrite dans la Charte de déontologie du 17 mai 2012 signée par tous les membres du Gouvernement dès le premier Conseil des ministres du quinquennat. Elle s'est ensuite traduite dans les décisions prises lors des Comités interministériels pour la modernisation de l'action publique des 18 décembre 2012, 2 avril 2013, 17 juillet 2013 et 18 décembre 2013, mais aussi par l'adoption lors du séminaire gouvernemental sur le numérique du 28 février 2013 d'une ambitieuse feuille de route stratégique. C'est également un engagement porté par la France avec l'adoption le 18 juin 2013, par les chefs d'État et de Gouvernement du G8, de la Charte du G8 pour l'ouverture des données publiques. Par ailleurs, la France a rejoint le « Partenariat pour le gouvernement ouvert » dont elle prendra la présidence à l'automne 2016. Dans ce cadre, elle a remis son plan d'action national 2015-2017, qui comprend plusieurs engagements relatifs à l'ouverture des données.

1.3 Eléments de droit comparé

La Finlande est un exemple intéressant d'accès libre et ouvert aux documents administratifs et aux données publiques. L'accès aux archives publiques y est garanti juridiquement depuis la loi Access to Public Records de 1766. La Finlande a ouvert en 1951 le droit d'accès aux documents administratifs avec la loi sur la Publicity of Official Documents. C'est en 1999 que sont établies les bases juridiques de l'ouverture des données par défaut avec la loi sur l'Openness of Government Activities (n° 621/1999), modifiée en 2002 par la loi n° 1060/2002. Cette loi introduit un principe d'ouverture selon lequel tous les documents officiels sont libres de droit sauf indication contraire. Cette qualification déclenche automatiquement non seulement le droit d'accès aux documents, mais aussi l'obligation pour les autorités d'en promouvoir l'accès, la diffusion et de mettre en place de bonnes pratiques de gestion de l'information. La loi prévoit que cette diffusion doit être libre et facile et qu'elle peut avoir lieu en ligne.

La Grèce a consacré dans la loi de 2013 du « Transparency Program » l'obligation pour les autorités de diffuser activement les données publiques, au-delà des demandes individuelles d'accès à l'information. Cette loi oblige ainsi le Gouvernement à publier en ligne un ensemble de données administratives, juridiques, budgétaires et géographiques (22 domaines spécifiques). La loi prévoit que ces actes et décisions administratives ne deviennent valides qu'après avoir été publiés en ligne. Aussi, selon cette législation, les documents téléchargés ont-ils statut de version officielle et prévalent sur le reste des versions disponibles.

2. Objectifs poursuivis

Le présent projet de loi vise à augmenter le volume de documents administratifs mis en ligne par les administrations dans le cadre de la politique d'open data, afin d'accroître la transparence des autorités publiques, d'améliorer les services publics et de stimuler le développement de nouvelles activités économiques.

A cette fin, le projet de loi élargit les obligations de diffusion spontanée des documents administratifs prévues aux articles L. 312-1 et L. 312-2 du code des relations entre le public et l'administration. L'article concerne des documents qui étaient déjà communicables à tous aujourd'hui en application du droit d'accès aux documents administratifs, mais qui devaient être expressément demandés par les citoyens : ces documents devront désormais être publiés d'office par les administrations et seront ainsi plus largement accessibles.

L'article prévoit ainsi quatre nouvelles obligations de diffusion publique en ligne pour les documents administratifs disponibles sous format électronique et qui sont déjà communicables à toute personne en application du droit d'accès aux documents administratifs :

a) Diffusion des documents communiqués par l'administration à la suite d'une demande formulée par une personne privée ;
b) Diffusion des principaux documents détenus par chaque administration, qui doivent déjà être répertoriés aujourd'hui en vertu de l'article 17 de la loi du 17 juillet 1978 ;
c) Diffusion des bases de données produites ou reçues par chaque administration ainsi que de leur contenu ;
d) Diffusion des données dont la publication présente un intérêt économique, social ou environnemental.

Cette avancée aura pour conséquence de limiter la communication sur demande des documents administratifs existant sous format électronique, qui seront rendus librement accessibles par Internet.

Avec le numérique, l'administration entre dans une nouvelle logique, celle de la mise à disposition des données, dans laquelle elle doit avoir l'initiative de la transparence.

Cette politique constitue un axe essentiel de la construction d'un gouvernement plus ouvert et plus efficace. Il s'agit donc d'une dimension importante de la vie démocratique et de la modernisation de l'action publique. C'est aussi un important levier de stimulation du dynamisme économique et de l'innovation.

L'article 3, supprime les dispositions de l'article L. 312-1 du CRPA relatives à la publication de documents administratifs comportant des données personnelles ou des mentions couvertes

par les articles L. 311-5 et L. 311-6 : ces dispositions sont remplacées par celles introduites par le II de l'article 4, qui crée un nouvel article L. 312-1-2 du même code, ces dispositions s'insérant ainsi mieux dans le nouveau dispositif mis en œuvre par le projet de loi.

L'article 5 fixe les délais de mise en œuvre du nouveau dispositif et précise que les documents administratifs sont communiqués, et désormais diffusés, sous réserve des droits de propriété littéraire et artistique.

3. Nécessité de légiférer

La démarche suivie jusqu'ici par la politique française d'open data a reposé sur des outils non contraignants pour les administrations publiques. Malgré les succès obtenus, il est nécessaire désormais d'accroître les obligations légales pesant sur les administrations pour franchir une nouvelle échelle dans la diffusion en ligne des informations publiques qu'elles détiennent.

Dans la mesure où ces dispositions modifient la partie législative du code des relations entre le public et l'administration, le recours à la voie législative est nécessaire.

4. Analyse des impacts des dispositions envisagées

4.1 Impacts économiques et sociaux

Selon le rapport établi par Graham Vickery[2], l'ouverture des données publiques au sein de l'union européenne aurait généré une activité économique directe (réutilisation) de 32 Md€ en 2010. Le même rapport évaluait l'impact économique agrégé direct et indirect d'une ouverture plus large des données publiques et d'un accès facilité à ces données à environ 200 Md€ annuels (soit 1,7% du PIB européen). Au Royaume-Uni, l'un des pays en pointe de l'ouverture des données publiques, une étude indépendante chiffrait à 1,8 Md£ (0,1% du PIB britannique) le gain économique annuel direct du programme gouvernemental « open data », et à 6,8 Md£ les gains directs et indirects (0,4% du PIB britannique)[3].

L'ouverture des données (open data) génère de la valeur économique et sociale à travers quatre mécanismes principaux[4] : l'efficience par la réduction des coûts de transaction, l'innovation, la réduction des asymétries d'information et la collaboration.

- L'open data permet tout d'abord une meilleure utilisation, par les acteurs publics et privés, des ressources disponibles. Toute transaction économique engendre des coûts liés à sa réalisation (coût de recherche d'information notamment). En mettant à disposition librement et gratuitement les données publiques, on réduit ces coûts de transaction, tant dans leur phase amont que dans la transaction elle-même. La gratuité des données et leur mise à disposition dans des formats libres et ouvertes via une plateforme accessible à tous (par exemple data.gouv.fr) est source d'efficience et d'efficacité, tant pour les administrations que pour les acteurs privés. Plusieurs

[2] Review of recent studies on PSI re-use and related market developments, Graham Vickery, 2008
[3] An independant review of public sector information, Shakespeare Review, 2013
[4] « The Generative Mechanisms of Open Government Data », European Conference on Information Systems, Jetzek, Avital, Michel, 2013

expériences viennent étayer ce mécanisme de création de valeur. En Australie, les coûts de transaction induits par la vente et la distribution des données géographiques australiennes a été évalué, avant leur mise à disposition libre et gratuite en 2002, entre 17% et 33% des revenus. Le gain annuel de cette ouverture a été évalué à 1,7 million de dollars par an pour la seule réduction des coûts de transaction[5]. Au Danemark, le gouvernement a lancé un programme nommé « Basic Data ». Il s'agit de mettre en place une infrastructure informationnelle autour de trois bases de données de référence (registres-clés), librement et gratuitement disponibles. Les gains de ce projet sont estimés à 35 millions d'euros annuels pour le secteur public (meilleure efficience) et 70 millions d'euros pour le secteur privé[6]

- Le second mécanisme de génération de valeur est lié à l'utilisation, par les secteurs public et privé, des données libres et ouvertes pour créer de nouveaux produits et services (innovation). Aux Pays-Bas, l'ouverture des données météorologiques a permis la création d'un écosystème de ré-utilisateurs professionnels très dynamique: le revenu des acteurs privés a augmenté de 400%, le nombre d'utilisations de ces données de 300%. Au final, ces activités ont généré un retour de 35 millions d'euros pour les finances publiques néerlandaises, sous la forme d'impôts et de taxes additionnels[7].

  Plusieurs études européennes montrent que la baisse d'une redevance ou sa suppression entraîne mécaniquement une augmentation de la réutilisation des données concernées[8]. Par exemple, le passage à la gratuité du référentiel à grande échelle de l'IGN pour les organismes chargés d'une mission de service public administrative, a entraîné une multiplication par 20 des volumes de données téléchargées, soit un bénéfice social estimé à 114 M€/an, pour un manque à gagner de 6 M€/an de redevances environ.[9]

- Le troisième mécanisme générateur de valeur est lié à la réduction de l'asymétrie d'information par une plus grande transparence. Il y a asymétrie d'information quand un acteur possède une information plus complète, ou de meilleure qualité, que les autres acteurs participant à une transaction ou une communication. Cela aboutit à des situations non optimales. Les données ouvertes permettent de réduire ces asymétries à plusieurs niveaux. Au niveau macroéconomique, la transparence est un outil de lutte contre la corruption reconnu notamment par la Banque mondiale. Au niveau microéconomique, la mise en ligne de données sur les marchés publics permet à tous les acteurs de disposer du même niveau d'information. Les répondants peuvent connaître le dernier attributaire d'un marché public et les conditions du marché, leur permettant ainsi de mieux dimensionner leur réponse. Le nombre et la qualité des réponses peut être supérieure, ce qui est aussi une condition d'efficacité de l'achat public.

[5] « Re-use of public sector information. Report for Danish Ministry for Housing, Urban and Rural Affairs », Marc de Vries, 2012
[6] « Good Basic Data for Everyone – A Driver for Growth and Efficiency », Digitaliseringsstyrelsen, 2012
[7] Marc de Vries, op. cit.
[8] «Review of Recent Studies on PSI Re-Use and Related Market Developments» - Graham Vickery, 2010.
[9] Mission redevances, Adnène Trojette 2013

- Enfin, l'open data crée les conditions d'une collaboration entre de multiples acteurs, tant publics que privés. La collaboration génère des économies d'échelle. Ainsi, la plateforme data.gouv.fr permet à chacun d'enrichir, d'améliorer et de repartager un jeu de données. Depuis fin 2013, de nombreux exemples d'enrichissement ont été documentés. Le fichier des accidents corporels de la circulation a fait l'objet de multiples améliorations par les ré-utilisateurs : nettoyage, correction des doublons, ajout des codes géographiques (INSEE et codes postaux). De même, les utilisateurs du site ont pu signaler les erreurs aux producteurs et proposer des corrections (signalement d'erreurs de géocodage, d'adresses absentes ou incomplètes, de données manquantes), enclenchant ainsi une dynamique d'amélioration continue de la qualité des données.

4.2 Impacts sur les administrations de l'État

A titre liminaire, il convient de préciser que les nouvelles obligations pour les administrations de diffuser en ligne leurs documents et données ne les contraignent en aucune manière à numériser leurs documents sur support papier. En effet, le projet d'article 4 prévoit expressément que les documents sont diffusés publiquement en ligne uniquement "lorsqu'ils sont disponibles sous forme électronique". Ceci est tout à fait en cohérence avec les règles actuellement en vigueur, le droit d'accès aux documents administratifs n'ayant ni pour objet ni pour effet de contraindre l'administration à établir un document nouveau pour répondre à une demande ou, en l'occurrence, pour en assurer la diffusion. Le document doit ainsi exister en l'état ou pouvoir être obtenu par un traitement automatisé d'usage courant :

- *Le document doit exister en l'état* : le Conseil d'État, dès le début des années 1980, avait posé le principe selon lequel le droit à communication posé par l'article 2 de la loi du 17 juillet 1978 ne s'appliquait qu'à des documents existants. Par conséquent l'administration n'est tenue, lorsqu'elle est saisie d'une demande tendant à la communication d'un dossier qui n'existe pas en tant que tel, ni « de faire des recherches en vue de collecter l'ensemble des documents éventuellement détenus »[10], ni d'établir un document en vue de procurer les renseignements ou l'information souhaités[11]. La communication peut donc être refusée s'agissant de documents à confectionner, par le biais d'un traitement quelconque, de recherches, d'une synthèse, d'une analyse[12].
- *ou pouvoir être obtenu par un traitement automatisé d'usage courant* : depuis la loi relative aux droits des citoyens dans leurs relations avec les administrations (DCRA) du 12 avril 2000, l'article 1er de la loi de 1978 impose la communication lorsque le document n'existe pas en l'état mais peut être obtenu par un traitement automatisé d'usage courant (avis CADA n° 20001636 du 25 mai 2000) : il s'agit des documents obtenus en ayant recours à un programme informatique de maniement aisé et à la disposition du service qui détient la base de données. L'ordonnance de 2005 a modifié la formulation de l'article 1er sans changer le droit applicable : celui-ci mentionne désormais les documents « quel que soit le support utilisé pour la saisie, le stockage ou la transmission des informations qui en composent le contenu ». Cette modification

[10] CE, 27 septembre 1985, Ordres des avocats de Lyon c/ Bertin, n°56543
[11] Avis CADA, 8 janvier 1987, Thomas, 5e rapport page 109 - CE, 30 janvier 1995, Min. d'État, min. éduc. nat. c/ Mme Guigue et CE, 22 mai 1995, Association de défense des animaux victimes d'ignominie ou de désaffection
[12] CE, Association SOS Défense, 9 mars 1983, Lebon p. 728

n'a modifié en rien la position de la CADA qui apprécie toujours l'existence du document en vérifiant s'il peut être obtenu par un traitement automatisé d'usage courant. En revanche, dès lors que les informations sollicitées doivent, pour être extraites d'un fichier informatique, faire l'objet de requêtes informatiques complexes ou d'une succession de requêtes particulières qui diffèrent de l'usage courant pour lequel ce fichier a été créé, l'ensemble des informations sollicitées ne peut être regardé comme constituant un document administratif existant (conseil CADA n° 20133264 du 10/10/2013). Le caractère complexe du traitement pourra s'apprécier au regard du temps passé par les agents à le concevoir (conseil 20141989 du 18/09/2014).

L'article 4 du projet de loi s'inscrit pleinement dans le dispositif fixé par cette jurisprudence, qu'il n'a aucunement vocation à modifier.

Ainsi, ne saurait être soumise à l'obligation de diffusion une base de données contenant des données personnelles dont l'anonymisation, qui peut s'avérer parfois extrêmement complexe, excèderait un traitement automatisé d'usage courant. D'autres procédés d'anonymisation, au contraire, n'iront pas au-delà d'un traitement automatisé d'usage courant dès lors qu'il suffira uniquement d'occulter un champ.

A ce propos, concernant l'obligation de publication de documents administratifs dans un standard ouvert aisément réutilisable, et si l'on prend pour exemple les documents créés par un logiciel de traitement de texte, soit le document existe en l'état dans ce standard, tel que le préconise d'ores et déjà le référentiel général d'interopérabilité qui s'impose à l'ensemble des autorités administratives, soit il est dans un format dit "propriétaire". Dans ce cas, la conversion du format "propriétaire" en standard ouvert aisément réutilisable, pourra très facilement être réalisée de façon unitaire ou par lots (grâce à une macro simple à mettre en œuvre) à l'aide d'un logiciel gratuit, soit à l'aide d'un logiciel payant (quelques dizaines d'euros) qui pourra en quelques clics convertir par lots de nombreux documents. Dans un cas comme dans l'autre, cette conversion devra toujours être regardée comme un traitement automatisé d'usage courant.

En ce qui concerne la publication, les nouvelles obligations des documents administratifs prévues par le présent article seront mises en œuvre facilement au plan technique grâce à la plateforme ouverte des données publiques, data.gouv.fr. Cette plateforme est déjà mise aujourd'hui à disposition des administrations d'État, des opérateurs et des collectivités locales pour la diffusion publique en ligne de leurs données. Quelques minutes suffisent pour créer le compte d'une organisation et mettre en ligne (en l'hébergeant ou en référençant une URL existante) un jeu de données. Data.gouv.fr accueille aujourd'hui près de 21 000 jeux de données, issus de 350 producteurs différents, dont les ministères, les grands producteurs (IGN, INSEE, Meteo-France) et les collectivités territoriales.

Par ailleurs, la diffusion pourra en outre être effectuée par une mise en ligne sur le site internet de l'administration concernée, ou sur une autre plateforme dédiée (telle que les portails open data propres créés par un certain nombre de collectivités locales ou d'organismes publics). La mission Etalab met également à disposition un guide de publication à destination des administrations.

La circulaire du 26 mai 2011 relative à la création du portail data.gouv.fr prévoit, dans son annexe IV, que chaque ministère désigne un interlocuteur unique pour la mission Etalab afin

de faciliter le recensement et la transmission des informations publiques de son administration. Cette personne est placée sous l'autorité directe et immédiate du secrétaire général du ministère. Le réseau des correspondants « Open Data » est animé par la mission Etalab, qui les réunit sur une base mensuelle.

De même que les administrations centrales, les services déconcentrés de l'État peuvent aisément partager leurs données sur la plateforme data.gouv.fr en quelques clics seulement. Ces données peuvent être hébergées ou uniquement référencées par le site à partir de plateformes existantes.

En particulier, une passerelle a été mise en place pour référencer automatiquement les données environnementales et géographiques concernées par les 34 thématiques de la Directive européenne Inspire[13], qui pousse les très nombreux systèmes d'information géographique d'Europe à converger vers les mêmes standards pour faciliter la circulation et l'interopérabilité des données. Son large périmètre porte sur de nombreuses données de Directions Départementales des Territoires (DDT) ou de Directions Régionales de l'Environnement, de l'Aménagement et du Logement (DREAL), qui sont ainsi déjà présentes sur la plateforme.
Enfin on peut considérer que la diffusion progressive des principales bases de données existant au niveau national, généralement alimentées à partir des données collectées ou renseignées par les services déconcentrés de l'État, n'induira pas de charge supplémentaire pour eux.

Faisabilité de l'utilisation de standards ouverts

En application du présent article, les administrations publiques devront publier des documents dans un standard ouvert aisément réutilisable.

Il convient tout d'abord de différencier le "standard[14]" de la "norme", cette dernière étant publiée par un organisme de normalisation officiellement agréé par un État, ce qui n'est pas toujours le cas du "standard".

Le présent projet de loi privilégie les termes de "standard ouvert" à ceux de "format ouvert" pour plusieurs raisons.

Tout d'abord, le terme de "format" apparaît comme plus générique que "standard", qui est plus précis et qui, de plus, bénéficie d'une définition légale dans l'article 4 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique. Au sens de cette loi, "On entend par standard ouvert tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre."

[13] http://www.developpement-durable.gouv.fr/IMG/pdf/Themes_Inspire.pdf
[14] La langue anglaise ne marque pas la différence entre norme et standard (« norme » se dit « *standard* » en anglais), on parle pour les normes de standards *de jure* et pour les simples standards de standards *de facto*. Un simple standard (*de facto*) est généralement déterminé soit par un industriel pionnier ou en position dominante sur un marché, soit par une association professionnelle ou un consortium d'acteurs industriels (comme IEEE ou OASIS).

Par ailleurs, les termes de "standard ouvert" sont consacrés dans le référentiel général d'interopérabilité (RGI), qui s'applique à l'ensemble des autorités administratives, en vertu de l'ordonnance du 8 décembre 2005 et du décret n° 2007-284 du 2 mars 2007. Les systèmes d'information doivent donc déjà être mis en conformité avec le RGI, qui prévoit notamment le recours à des standards ouverts. La notion de format « réutilisable » ne recouvre pas entièrement celle de format ouvert. En effet, du point de vue du RGI, le PDF est un standard ouvert, mais en pratique la réutilisation des données contenues dans un PDF est très difficile. Par contre, le même RGI recommande l'usage du format Open Document plutôt que le format concurrent proposé par Microsoft.

Enfin, le "standard", qui emporte à la fois les notions d'élément de référence, de règle ou de modèle, sous-entend une large adhésion et l'emploi par une grande communauté d'acteurs et est, en soi, porteur d'interopérabilité et de facilité de réutilisation, là où le "format ouvert" reste extrêmement générique et peut tout à fait n'être utilisé que par une partie marginale de l'écosystème et être, de fait, d'une réutilisation beaucoup moins aisée.

4.3 Impact sur les collectivités territoriales

La loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République, dite loi NOTRe, a créé, par son article 106, de nouvelles obligations pour les collectivités territoriales et les communes de Nouvelle-Calédonie relatives à la transparence de leurs données.

Ainsi, les collectivités territoriales, et les communes de Nouvelle-Calédonie, de plus de 3 500 habitants ainsi que les établissements publics de coopération intercommunale à fiscalité propre auxquels elles appartiennent sont tenues de rendre accessibles en ligne les informations publiques mentionnées à l'article 10 de la loi n° 78-753 du 17 juillet 1978, lorsque ces informations se rapportent à leur territoire et sont disponibles sous forme électronique. Il est en outre précisé, que ces informations publiques sont offertes à la réutilisation dans les conditions prévues au chapitre II du titre Ier de la loi du 17 juillet 1978 précité.

Dans ces conditions, et dans la mesure où les dispositions prévues par l'article 106 de la loi NOTRe sont tout à fait à même de répondre aux objectifs fixés par l'article 3 du projet de loi, les collectivités territoriales et les communes de Nouvelle-Calédonie ainsi que les EPCI à fiscalité propres sont exclus du dispositif, le projet de loi ne créant aucune obligation nouvelle pour ces administrations.

En outre, pour tenir compte des difficultés de mise en œuvre que les règles prévues par le projet d'article 4 pourraient présenter pour les administrations dotées de moyens humains limités, une exclusion est également prévue pour les personnes morales publiques ou privées de petite taille, définies comme ayant un nombre d'agents ou de salariés inferieur à 250. Le seuil retenu permet de garantir que seuls des organismes disposant d'un service informatique suffisamment structuré pour mettre en œuvre les nouvelles obligations de publication y seront soumis. Cette disposition permettra notamment de ne pas inclure dans le champ d'application du présent article les établissements publics locaux de petite taille, en cohérence avec l'exclusion des collectivités territoriales les plus petites du champ d'application de l'article 106 de la loi NOTRe. En ce qui concerne les organismes de droit privé chargés d'une mission de service public, le seuil retenu correspond au seuil de déclenchement de plusieurs obligations déjà prévues par le droit du travail ou le droit fiscal (par exemple les dispositions de l'article 230 H du code général des impôts).

5. Consultations menées

Le Conseil national d'évaluation des normes et la Commission d'accès aux documents administratifs ont été consultés.

6. Textes d'application et outre-mer

Un décret en Conseil d'État fixera les modalités d'applications de l'article 4.
La date mentionnée à l'article 5 sera fixée par voie de décret.

L'article 46 du projet de loi rend les présents articles applicables en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

Article 6
Principe de libre réutilisation des données pour les SPIC

1. État des lieux

L'ordonnance du 6 juin 2005 prise pour la transposition de la directive 2003/98/CE du 17 novembre 2003 avait supprimé le principe d'interdiction de réutilisation commerciale des documents administratifs posé par l'ancien article 10 de la loi du 17 juillet 1978 et créé le chapitre II reconnaissant explicitement le principe de libre réutilisation des informations publiques. La nouvelle rédaction de l'article 10 a affirmé le principe de libre réutilisation de ces informations « *par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus* ».

Cette formulation exclut du champ d'application de ce principe de libre réutilisation trois types d'informations : celles dont la communication ne constitue pas un droit (sauf si elles font l'objet d'une diffusion publique), celles produites ou reçues par les administrations dans l'exercice d'une mission de service public à caractère industriel ou commercial, enfin celles sur lesquels des tiers détiennent des droits de propriété intellectuelle.

Du point de vue de la communication des données, le régime des SPIC peut donc être qualifié d'hybride. Les organismes chargés de la gestion d'un SPIC font partie, quel que soit leur statut, des « administrations » au sens de l'article L. 300-2 du code des relations entre le public et l'administration, régies par le droit de communication des documents administratifs. Tous les documents produits ou reçus dans le cadre de leur mission de service public doivent être communiqués à quiconque en fait la demande – sous réserve des exceptions énumérées par les articles L. 311-5 et L. 311-6, notamment les documents dont la communication porterait atteinte au secret industriel et commercial, exception qui joue un rôle important pour les SPIC. Alors que pour les services publics administratifs, le droit de communication coïncide avec la liberté de réutilisation, il en est dissocié pour les SPIC en raison de l'exception b) prévue à l'article 10 de la loi du 17 juillet 1978. L'exclusion des données des SPIC limite fortement le champ des réutilisations d'informations publiques, réduisant ainsi les bénéfices potentiels de la politique d'open data.

Par ailleurs, l'article 10 de la loi prévoit que l'échange d'information entre les autorités, aux fins de l'exercice de leur mission de service public, ne constitue pas une réutilisation au sens de la loi du 17 juillet 1978, c'est-à-dire que les conditions de réutilisations posées par le chapitre II de la loi du 17 juillet 1978 ne s'appliquent pas aux autorités.

2. Objectifs poursuivis

Les deux objectifs de l'ouverture des données publiques, la transparence de l'action publique et le développement économique, sont aussi pertinents pour les SPIC que pour les SPA. Pour le citoyen, il est aussi intéressant de savoir comment sont rendus les services publics de transport ou de distribution de l'eau que ceux de l'éducation ou de la police. Du point de vue du développement économique, les données des SPIC ont une valeur certaine, puisqu'elles touchent à des services essentiels utilisés par l'ensemble de la population. En outre, à la différence des SPA, le développement économique entre dans l'objet même des SPIC : si la puissance publique décide de prendre en charge une activité de nature industrielle ou commerciale, c'est parce qu'elle estime que son intervention sera favorable au développement

économique de la collectivité. Dans la mesure où l'ouverture des données favorise le développement de nouvelles activités, elle entre pleinement dans la vocation des SPIC. Plusieurs SPIC, comme la SNCF, la RATP ou le Centre des musées nationaux, se sont d'ailleurs engagés de manière volontaire dans des démarches d'ouverture des données.

Le présent article vise donc à autoriser la réutilisation des informations publiques produites ou reçues dans le cadre des missions de service public industriel ou commercial. A cette fin, il prévoit un principe général de libre réutilisation des informations publiques des SPIC.

Champ d'application du dispositif juridique proposé

L'objectif poursuivi par l'ensemble du projet de loi consiste à créer un cadre législatif plus cohérent. Cette simplification se déroule en deux étapes :

- Premièrement, il s'agit d'harmoniser le champ des documents administratifs librement communicables et celui dont l'État, les collectivités territoriales et les personnes morales de droit public ou de droit privé chargées d'une mission de service public doivent, spontanément, assurer la diffusion.
- Dans ce cadre, la suppression de la deuxième exception est justifiée dans la mesure où les documents produits ou reçus par les personnes mentionnées à l'article 1er de la loi dans l'exercice d'une mission de service public à caractère industriel ou commercial revêtent effectivement un caractère administratif (voir par exemple, pour la SNCF, avis CADA n° 20141034 du 10 avril 2014) et doivent donc pouvoir être réutilisés dans les mêmes conditions que les autres documents administratifs.

D'autre part, le projet de loi réaffirme le principe selon lequel l'ensemble des informations publiques qui ont été communiquées ou diffusées sont librement réutilisables à d'autres fins que la mission de service public pour laquelle elles ont été produites ou reçues. Ce principe rappelle que sont réutilisables les informations qui sont accessibles, soit par la communication, soit par la diffusion publique.

Il convient d'ajouter que le nouveau dispositif proposé respecte l'adage *Specialia generalibus derogant, non generalia specialibus*, selon lequel les règles spéciales dérogent aux règles générales. Même si les règles générales prévues par l'actuel projet de loi sont postérieures à certaines dispositions spéciales préexistantes, le présent projet n'a ni pour objet, ni pour effet de les abroger. Ainsi, l'article 4 de la loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques, qui a instauré des règles d'accès aux données nécessaires à l'information du voyageur créant ainsi un régime spécifique de l'open data dans le domaine des transports ne se verra pas impacté par les dispositions du présent article.

3. Analyse des impacts des dispositions envisagées

3.1 Impacts généraux

Les SPIC peuvent être assurés par quatre catégories de personnes :

- L'État, les collectivités territoriales ou leurs groupements, qui les exploitent directement sous la forme d'une régie.

- Les établissements publics industriels et commerciaux (EPIC), qui sont placés sous la tutelle de l'État ou d'une collectivité territoriale. Parmi les EPIC nationaux, on trouve certaines grandes entreprises publiques ayant conservé ce statut (SNCF, RATP, les grands ports maritimes), des institutions culturelles (Opéra de Paris, Comédie française, Centre des musées nationaux), des institutions financières publiques (Bpifrance, AFD) et des institutions nationales diverses telles que le CEA, le CNES ou encore l'ADEME.

- Les personnes de droit privé gérant un service public dans le cadre d'une relation contractuelle avec une personne publique. Ce contrat peut être un marché de service public, lorsque la rémunération de la personne privée est assurée principalement par le paiement d'un prix, ou une délégation de service public (DSP), lorsque la rémunération est substantiellement liée aux résultats du service. Dans le cadre de la transposition de la directive 2014/23/UE du Parlement européen et du Conseil du 26 février 2014 sur l'attribution des contrats de concession, il est prévu de remplacer la notion de DSP par celle de concession de service public, dont la définition resterait proche.

- Les personnes de droit privé gérant un service public en vertu d'une disposition législative ou réglementaire. C'est notamment le cas d'anciens EPIC devenus des entreprises de droit privé, comme La Poste ou EDF.

Pour toutes ces catégories, le SPIC se distingue du service public administratif, selon la jurisprudence du Conseil d'État (CE Ass., 16 novembre 1956, Union syndicale des industries aéronautiques), par la réunion de trois caractéristiques qui l'apparentent à une entreprise : l'objet du service, l'origine des ressources et les modalités de son organisation et de son fonctionnement.

Le présent article rend possible la réutilisation des informations publiques librement communicables pour l'ensemble des personnes morales exerçant une mission de service public industriel et commercial : ces personnes n'auront plus le droit d'interdire la réutilisation des informations publiques qu'elles communiquent.
Ainsi, cet article permet la totale harmonisation des règles de réutilisation applicables à toutes les autorités chargées d'une mission de service public, qu'elle soit de nature administrative ou industrielle et commerciale.

Toutefois, dans la mesure où ne sont pas concernées les informations dont la communication ne constitue pas un droit en application du chapitre I^{er} de la loi du 17 juillet 1978, et notamment du fait des dispositions prévues à l'article 6 de ladite loi, la réutilisation est rendue possible sans méconnaitre les secrets protégés par la loi et notamment le secret en matière commerciale et industrielle.

3.2 Impacts sur les collectivités territoriales

Un nombre importants de services publics industriels et commerciaux relèvent des collectivités territoriales :

- La gestion directe par une régie est assez répandue pour un certain nombre de services publics locaux, notamment communaux, par exemple dans les domaines de l'eau, des transports, de la culture ou des pompes funèbres ;
- De nombreux EPIC locaux dépendent des collectivités territoriales : on peut notamment mentionner les offices publics de l'habitat, les établissements publics

fonciers locaux, les établissements publics d'aménagement ou encore les offices de tourisme n'ayant pas la forme associative.

Ces SPIC locaux sont inclus dans le champ d'application du présent article, mais son impact sur les collectivités territoriales et leurs organismes est limité par le champ d'application des nouvelles obligations de publication des données publiques :

- Les collectivités territoriales de moins de 3 500 habitants et leurs EPCI à fiscalité propre sont exclus du principe d'open data par défaut en vertu de l'article 106 de la loi NOTRe ;
- Les personnes publiques ou privées de petite taille sont exclues des nouvelles obligations de publication prévues par l'article 1er du présent projet de loi.

En conséquence, de nombreux SPIC locaux ne seront pas soumis à de nouvelles obligations de publication de leurs données publiques, ce qui réduira pour eux la portée du nouveau droit à la réutilisation des informations publiques prévu par le présent article.

4. Consultations menées

Le Conseil national d'évaluation des normes et la Commission d'accès aux documents administratifs ont été consultés.

5. Outre-mer

L'article 10 de la loi n° 78-753 du 17 juillet 1978 est rendu applicable en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna par l'article 59 de cette loi. L'article 46du projet de loi rend applicables en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises les modifications apportées à l'article 10 de la loi du 17 juillet 1978 par le présent projet de loi.

Article 7
Rationalisation du régime de réutilisation des informations publiques

1. État des lieux

1.1 Articulation avec le droit sui generis - Dérogation au droit des bases de données pour les organismes publics

La directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données a été transposée dans notre droit national dans le code de la propriété intellectuelle. La protection spécifique accordée au producteur d'une base de données peut constituer, dans bien des cas, un obstacle rendant impossible la réutilisation des informations issues de ces bases.

En effet, l'article L. 342-1 du code de la propriété intellectuelle prévoit que : *« Le producteur de bases de données a le droit d'interdire :*

1° L'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;

2° La réutilisation, par la mise à la disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme. »

L'article L. 342-2 ajoute : *« Le producteur peut également interdire l'extraction ou la réutilisation répétée et systématique de parties qualitativement ou quantitativement non substantielles du contenu de la base lorsque ces opérations excèdent manifestement les conditions d'utilisation normale de la base de données. »*

Ces dispositions du code de la propriété intellectuelle peuvent aller à l'encontre du principe de libre réutilisation des données publiques encouragé par le présent projet de loi. La Cour administrative d'appel de Bordeaux dans sa décision du 26 février 2015 « Notrefamille.com » a ainsi jugé qu'un conseil départemental pouvait empêcher la réutilisation d'une base de données détenue par son service des archives au nom du droit *sui generis* prévu à l'article L. 342-1 du code de la propriété intellectuelle.

1.2 Encadrement des licences pouvant être utilisées par les administrations

La Circulaire du 26 mai 2011 relative à la création du portail unique des informations publiques de l'État « data.gouv.fr » par la mission « Etalab » et l'application des dispositions régissant le droit de réutilisation des informations publiques prévoyait qu'une licence de réutilisation serait élaborée par Etalab et par *« un groupe de travail composé de l'Agence du patrimoine immatériel de l'État (APIE), du Conseil d'orientation de l'édition publique et de l'information administrative (COEPIA) et des administrations concernées »*. Depuis novembre 2011, la licence ouverte[15] s'impose ainsi aux administrations de l'État.

Cette même circulaire prévoyait également que des licences gratuites spécifiques pouvaient être toutefois adoptées dans les cas où la réutilisation d'un jeu de données déterminé ferait l'objet de conditions particulières, et que les administrations concernées les élaboreraient et les soumettraient à « Etalab », qui les validerait et les publierait sur « data.gouv.fr ».

De nombreuses licences spécifiques ont toutefois pu proliférer, nuisant à la facilité de réutilisation et à la compréhension des conditions spécifiques imposées aux réutilisateurs.

2. Objectifs poursuivis

2.1 Articulation avec le droit sui generis - dérogation au droit des bases de données pour les organismes publics

Sans porter préjudice aux droits de propriété intellectuelle détenus par des tiers, le projet de loi prévoit d'adapter, pour les bases de données mises en œuvre par les administrations et qui

[15] https://www.etalab.gouv.fr/licence-ouverte-open-licence

doivent faire l'objet d'une diffusion publique, les droits que les administrations détiendraient au titre des articles L. 342-1 et L. 342-2 du code de la propriété intellectuelle de façon à ce qu'ils ne puisse constituer un obstacle à la réutilisation des informations contenues dans ces bases de données.

2.2 Encadrement des licences pouvant être utilisées par les administrations

La multiplication des licences accroît l'insécurité juridique lors de la réutilisation de données publiques. Par ailleurs, le type de licences utilisé modifie de manière importante les effets de l'ouverture des données. A titre d'exemple, la licence ODBL permet ainsi, en obligeant à un partage à l'identique, de s'assurer que les données ne sont pas refermées par leurs réutilisateurs et donc de décupler les bénéfices de l'ouverture des données publiques.

L'objet du présent article, en dressant la liste des licences gratuites que les administrations peuvent utiliser, est donc de faciliter la réutilisation des données publiques en rendant plus compréhensibles et conforme aux objectifs visés par la politique d'ouverture et de partage des données publiques les conditions de réutilisations des données, en encadrant les types de licence autorisées et en en limitant le nombre.

3. Nécessité de légiférer

3.1 Articulation avec le droit sui generis - dérogation au droit des bases de données pour les organismes publics

La présente disposition, qui s'applique tant aux administrations d'État, qu'à l'ensemble des autorités administratives constitue une dérogation aux dispositions législatives du code de la propriété intellectuelle concernant la protection accordée aux producteurs de bases de données.

3.2 Encadrement des licences pouvant être utilisées par les administrations

La présente mesure s'applique tant aux administrations de l'État qu'aux collectivités territoriales. Une disposition législative est nécessaire pour préciser un encadrement de l'utilisation des licences.

4. Analyse des impacts des dispositions engagées

4.1 Articulation avec le droit sui generis - Dérogation au droit des bases de données pour les organismes publics

Ces nouvelles dispositions permettront aux administrations de voir la situation de leurs bases de données clarifiée. En effet, beaucoup d'entre elles s'interrogent sur l'articulation du droit *sui generis* accordé aux producteurs de bases de données avec le droit de réutilisation prévu par la loi du 17 juillet 1978.

Impact sur les collectivités territoriales

Les collectivités territoriales bénéficieront de ce régime simplifié.

4.2 Encadrement des licences pouvant être utilisées par les administrations

Ces nouvelles dispositions permettront aux administrations de choisir aisément parmi les licences gratuites proposées et adaptées à leurs besoins.

Impact sur les collectivités territoriales

Les collectivités territoriales bénéficieront de ce régime simplifié avec la sécurité juridique liée à l'assurance que la licence figurant dans la liste est agréée.

5. Consultations menées

Le Conseil national d'évaluation des normes et la Commission d'accès aux documents administratifs ont été consultés.

6. Textes d'application et Outre-mer

Un décret fixera la liste des licences types pour les réutilisations à titre gratuit.

L'article 46 du projet de loi rend le présent article applicable en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

Article 8
Missions et pouvoirs de la CADA

Obligation d'actualiser chaque année le répertoire des principaux documents de chaque administration publique

1. État des lieux

L'article 17 de la loi du 17 juillet 1978 fait obligation à chaque administration publique mentionnée à l'article 1er de la même loi de publier un répertoire des principaux documents où figurent les informations publiques qu'elle détient.

La mise en œuvre de cette obligation a été prévue par la circulaire du Premier ministre du 29 mai 2006 (section 2) mais elle reste inégale selon les administrations publiques et trop peu effective de façon générale.

Les choix des différentes administrations pour établir le contenu de ce répertoire sont également hétérogènes, certains se limitant par exemple à des documents qui font déjà l'objet d'un processus de publication[16].

2. Objectifs poursuivis

En introduisant une obligation de mise à jour annuelle du répertoire prévu à l'article 17, cet article vise un double objectif :

- Rendre plus effective la publication d'un tel répertoire par chacune des administrations publiques soumises aux règles introduites par la loi du 17 juillet 1978 ;
- Rendre plus pertinent le contenu du répertoire publié, en garantissant son évolution régulière pour inclure les nouvelles informations publiques produites ou reçues l'administration.

3. Nécessité de légiférer

L'obligation introduite par cet article s'impose à toutes les personnes morales mentionnées à l'article L. 300-2 du code des relations entre le public et l'administration : État, collectivités territoriales, autres personnes publiques et personnes privées chargées d'une mission de service public.

Pour étendre cette obligation aux collectivités territoriales, à l'ensemble des personnes publiques et aux personnes privées chargées d'une mission de service public, il est nécessaire de passer par une modification législative.

---

[16] C'est le cas du répertoire des ministères économiques et financiers, qui recense l'intégralité des publications des ministères : http://www.economie.gouv.fr/cedef/repertoire-des-informations-publiques

4. **Analyse des impacts des dispositions envisagées**

La réforme permettra d'établir un processus de suivi régulier de la publication et de l'actualisation du répertoire prévu par l'article 17. Elle complète les dispositions du présent projet de loi qui rendent obligatoire la publication des documents contenus dans le répertoire, à compter d'une durée d'un après la promulgation du projet de loi.

La charge de travail pour les administrations publiques mentionnées à l'article L. 300-2 du code des relations entre le public et l'administration restera très limitée, s'agissant d'une obligation de mise à jour dont la périodicité est annuelle. Il convient de souligner que la nouvelle rédaction de l'article 17 de la loi CADA ne fait que préciser une règle déjà implicite dans la rédaction antérieure, à savoir que le répertoire n'est pas établi de façon immuable et définitive mais doit être mis à jour régulièrement.

Impact sur les collectivités territoriales

Cette disposition n'aura qu'un impact très limité sur les collectivités territoriales, selon les principes exprimés ci-dessus : une mise à jour annuelle pour préciser une obligation qui était déjà sous-jacente à l'actuelle rédaction de l'article 17 de la loi du 17 juillet 1978.

5. **Consultations menées**

La Commission d'accès aux documents administratifs a été consultée.

Création d'un droit de saisine de la CADA pour refus de publication d'un document administratif

1. **État des lieux**

Le troisième alinéa de l'article 20 de la loi du 17 juillet 1978 rend possible la saisine de la CADA par une personne à qui est opposé un refus de communication d'un document administratif en application du chapitre 1er de la même loi. Il n'est pas prévu en revanche qu'une personne puisse saisir la CADA pour un refus de publication d'un document administratif : si le document est communiqué mais non publié, la seule voie de recours est de saisir directement la juridiction administrative.

Cette situation se justifie par le caractère limité des obligations de publication des documents administratifs aujourd'hui prévues par le code des relations entre le public et l'administration qui prévoit une obligation de publication restreinte aux directives, instructions, circulaires, ainsi qu'aux notes et réponses ministérielles qui comportent une interprétation du droit positif ou une description des procédures administratives.

2. **Objectifs poursuivis**

Le présent projet de loi élargit les obligations de publication prévues par le code des relations entre le public et l'administration. Les administrations mentionnées à l'article L. 300-2 du même code devront désormais publier :

1° les documents qu'elles communiquent en application du chapitre 1er,
2° les documents mentionnés dans le répertoire prévu à l'article 17 de la loi du 17 juillet 1978,
3° les bases de données qu'elles produisent ou qu'elles reçoivent ainsi que leur contenu,
4° les données dont la publication présente un intérêt économique ou social.

Le présent article vise à faciliter la mise en œuvre de ces obligations nouvelles de publication. A cette fin, il ouvre la possibilité de demander un avis à la CADA en cas de refus de publication par une administration publique. Cette possibilité nouvelle permettra aux personnes privées de bénéficier de l'expertise spécialisée et de la rapidité de réponse de la CADA en cas de refus de publication d'un document. Cette réforme est donc de nature à rendre plus effectives les nouvelles obligations de publication des données publiques prévue par l'article 1er du présent projet de loi.

3. Nécessité de légiférer

Le présent article modifie l'article 20 de la loi du 17 juillet 1978 pour ouvrir un nouveau motif de saisine de la CADA. Le recours à la voie législative est donc nécessaire.

4. Analyse des impacts des dispositions envisagées

Selon les chiffres du rapport d'activité de la CADA pour 2013, la Commission a été saisie de 5486 dossiers dont 5306 demandes d'avis et 178 demandes de conseil. La nouvelle faculté de saisine de la CADA ouverte par le présent article pourrait théoriquement entraîner une hausse des demandes d'avis adressées à la CADA.

Toutefois, dans le même temps, les obligations accrues de publication des documents administratifs prévues par le présent projet de loi devraient permettre une baisse des demandes de communication de documents administratifs, et donc des saisines de la CADA à ce titre. En effet, conformément aux dispositions de l'article L. 311-2 du code des relations entre le public et les administrations, *« Le droit à communication ne s'exerce plus lorsque les documents font l'objet d'une diffusion publique ».*

En outre, le présent article prévoit la création d'une procédure simplifiée de réponse de la CADA aux demandes d'avis, qui lui permettra d'absorber une hausse éventuelle de ces demandes à moyens constants.

Aussi, on peut estimer que les différentes dispositions du projet de loi permettront d'aboutir à un point d'équilibre.

5. Consultations menées

La Commission d'accès aux documents administratifs a été consultée.

Possibilité de créer une procédure simplifiée de réponse aux demandes reçues par la CADA

1. **État des lieux**

La CADA est saisie d'un nombre croissant de demandes d'avis, qui ont le caractère d'un recours administratif obligatoire préalablement à la saisine du juge administratif. Le caractère collégial de la commission contribue à la qualité des avis qu'elle rend sur les questions les plus nouvelles ou les plus délicates.
Un examen collégial n'est cependant pas toujours indispensable, en particulier lorsque la commission ne peut faire autrement que de prendre acte de ce qu'une demande a perdu tout objet ou qu'il s'agit seulement de réitérer dans une affaire une réponse relevant de la doctrine bien établie de la commission, alors que le rythme des séances de la commission ralentit l'examen des demandes.

La commission a donc émis une recommandation de réforme dans son rapport annuel d'activité relatif à l'année 2013.

2. **Objectifs poursuivis**

Les objectifs poursuivis sont les suivants :

- Alléger la procédure suivie devant la commission et la charge de préparation de ses séances ;
- Raccourcir les délais effectifs de réponse aux demandes d'avis les plus simples ;
- Respecter le caractère collégial de la commission en la laissant maîtresse des délégations qu'elle accorderait.

3. **Nécessité de légiférer**

La répartition des compétences au sein d'un organe de l'État tel que la commission d'accès aux documents administratifs ne relève pas en principe du domaine de la loi défini par l'article 34 de la Constitution. Cependant, l'intervention du législateur pour donner un caractère collégial à la commission d'accès aux documents administratifs et en définir les attributions interdit que certaines de ces attributions soient exercées par le président de la commission, en l'absence dans la loi n° 78-753 du 17 juillet 1978 de disposition les lui confiant directement ou autorisant la commission à les lui déléguer, comme l'article 15 de la loi n° 78-17 du 6 janvier 1978 le permet au contraire en ce qui concerne la commission nationale de l'informatique et des libertés.

Sans modification des textes en vigueur, la seule alternative serait d'augmenter la fréquence des séances de la commission. Cette option contribuerait elle aussi à raccourcir les délais mais n'allégerait ni la procédure ni la charge de préparation des séances de la commission. En outre, elle imposerait, pour approcher d'un même résultat en termes de délais, de doubler la fréquence des réunions de la commission, ce qui paraît incompatible avec les moyens actuels de l'institution. Cette alternative paraît donc déraisonnable.

4. Analyse des impacts des dispositions envisagées

Evaluation des incidences de toute nature

- Pour les administrés, qui saisissent la commission : raccourcissement du délai de réponse aux demandes les plus simples, pour environ 20 % de l'ensemble des demandes, dans un premier temps.

- Pour les membres de la commission : allègement du même ordre de grandeur de l'ordre du jour des séances de la commission, permettant de consacrer plus d'attention aux affaires qui le méritent.

- Pour les agents permanents, les rapporteurs et le rapporteur général de la commission : réorganisation des circuits d'instruction de la même proportion des demandes d'avis, en vue de la simplification de ces circuits, meilleure répartition de la charge de travail par un allègement de la préparation des séances de la commission.

Impact sur les collectivités territoriales

Cette disposition ne crée aucune obligation ou charge nouvelle pour les collectivités territoriales, qui pourront en revanche bénéficier de cette procédure simplifiée.

Conditions de mise en œuvre de la réforme

Un décret d'application, pris en Conseil d'État, doit préciser les critères autorisant la commission à consentir une délégation à son président. La commission pourra prendre dans ce cadre une délibération accordant une telle délégation à son président.

5. Consultations menées

La Commission d'accès aux documents administratifs a été consultée.

6. Outre-mer

L'article 46 du projet de loi rend le présent article applicable en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

Section 2
Service public de la donnée

Article 9
Création d'un service public de la donnée

1. État des lieux

Aujourd'hui, dans la législation, la donnée est rarement considérée comme un objet autonome. On parle de « document » administratif, parfois d'information, mais pas de donnée en tant que telle[17]. Dès lors, la production comme la mise à disposition de ces données importantes pour le fonctionnement d'organisations publiques et privées ne sont aujourd'hui que le sous-produit d'un service public tiers ; par exemple, celui de la statistique publique ou celui de l'information légale.

2. Objectifs poursuivis

De multiples exemples montrent que les données jouent un rôle de plus en plus fondamental dans la création de valeur économique et sociale. C'est une des raisons qui fait que la France a mené, dans les dernières années, une politique active sur le ce plan : remarquée pour son action en matière d'open data (3e pays au monde pour le classement de l'Open Knowledge Foundation, en décembre 2014), elle a été le premier pays européen à se doter d'un administrateur général des données[18].

Au sein de l'ensemble des données produites par l'État, il convient d'identifier certaines données qui ont vocation à être érigés en « données de référence ». On entend par « données de référence » des données disponibles, largement diffusées et utilisée par une pluralité d'acteurs publics et privés, et dont la qualité est reconnue par l'État. C'est l'élargissement aux données, ressources immatérielles, d'une logique déjà à l'œuvre pour les ressources foncières, avec le cadastre.

L'enjeu est ici de constituer, dans un univers de données très dense et dont les sources ne sont pas toujours indentifiables ou maîtrisées, une ressource fiable et authentifiée par la puissance publique. A titre d'illustration dans le domaine informationnel, il n'existe qu'un seul identifiant pour une entreprise : son numéro SIRET. Les administrations sont tenues de l'utiliser[19]. Cet identifiant fait référence parce qu'il est utilisé par l'ensemble des acteurs dans leurs relations avec les entreprises ce qui ne fait que renforcer l'incitation à l'utiliser, confirmant, du même coup, la légitimité de cet identifiant.

L'objectif du service public de la donnée est d'organiser la production, la qualité et la circulation des données de référence en garantissant un niveau de qualité minimale dans leur diffusion.

---

[17] Premier alinéa de l'article premier de la loi n° 78-753 du 17 juillet 1978 : *« Le droit de toute personne à l'information est précisé et garanti par les dispositions des chapitres Ier, III et IV du présent titre en ce qui concerne la liberté d'accès aux documents administratifs. »*

[18] Décret n° 2014-1050 du 16 septembre 2014 instituant un administrateur général des données.

[19] Article R. 123-233 du code du commerce

Les **données de référence** sont identifiées et régies par des critères cumulatifs, qui reprennent des éléments du « Cadre commun d'architecture des référentiels de données » défini par la DISIC[20] :

1° *elles font l'objet d'une utilisation fréquente par un grand nombre d'acteurs tant publics que privés* : ces données ne sont pas produites pour une unique finalité d'usage, mais sont réutilisées par une vaste pluralité d'acteurs. Elles peuvent être utilisées par des métiers fondamentalement différents. Certaines données sur les entreprises sont par exemple utilisées aussi bien par les sphères fiscale, sociale, travail, emploi, développement durable, santé, agriculture…

2° *leur disponibilité et leur qualité, notamment leur précision, leur fréquence de mise à jour ou leur accessibilité sont critiques pour un grand nombre de processus pour les acteurs cités au 1°* : Ces données doivent ainsi exister (être produites), être précises et complètes (ex : « 64, boulevard Henri 4 » peut être nécessaire, « bd henri 4 » n'est pas équivalent), être disponibles et accessibles à tout moment et facilement, et être mises à jour fréquemment. A titre d'exemple, la mise à jour mensuelle d'une base peut rendre la donnée inaccessible pendant un temps donné, or cette indisponibilité peut mettre en péril des processus métiers qui ont besoin de s'y référer (par exemple des API entreprises utilisant le numéro de SIRET).

Dans le cadre des projets relatifs à la mise en œuvre de la stratégie de l'État Plateforme, plusieurs services utilisent des données considérées comme étant de référence. Les projets « marchés publics simplifiés » (MPS) et « aides publiques simplifiées» (APS) s'appuient sur la base SIRENE, le projet de système d'identification « France Connect » (FC) sur le répertoire national des individus et personnes physiques (RNIPP).

Ces deux référentiels (SIRENE et RNIPP) ont été créés et reposent actuellement sur une logique de fichier statique et fonctionnent sur un modèle de copie de fichier.

Or, les dispositifs MPS, APS ou FC nécessitent la donnée en temps réel et ne peuvent accepter, ce qui est arrivé à plusieurs reprises ces derniers mois, une indisponibilité de ces bases durant des périodes allant jusqu'à plusieurs heures avec des périodes de maintenance programmées durant les heures administratives ouvrées. Ceci est particulièrement sensible pour les matières où la contrainte de respect des délais pour l'utilisateur est primordiale comme c'est le cas pour les marchés publics.

Parmi les principales données de référence pourraient par exemple figurer :

- Le cadastre ;
- La base d'adresses nationale (BAN) collaborative ;
- Le référentiel à grande échelle (RGE) ;
- Le référentiel parcellaire graphique (RPG) ;
- Le registre des entreprises (SIRENE) ;
- Le registre national des associations (RNA) ;

[20] https://references.modernisation.gouv.fr/sites/default/files/Cadre%20Commun%20d%27Architecture%20des%20R%C3%A9f%C3%A9rentiel%20de%20donn%C3%A9es%20v1.0_0.pdf

3. Nécessité de légiférer

Dans la mesure où le présent projet de loi prévoit que toutes les autorités administratives concourent à la mission du service public créé par ce même article, et notamment les collectivités territoriales, le recours à la loi est justifié par le principe constitutionnel de libre administration des collectivités territoriales défini par les articles 34 et 72 de la Constitution.

Le dispositif est complété par des mesures de nature règlementaire. Les modalités d'application de cet article seront fixées par décret en Conseil d'État qui déterminera, le cas échéant, les modalités de coordination entre plusieurs administrations responsables de la production et de la diffusion de données de référence ainsi que les critères qualitatifs de ces données et les modalités de participation des collectivités territoriales au service public de la donnée.

Un décret simple déterminera la liste des données de référence et des administrations chargées de leur production et diffusion. Des arrêtés ministériels pourront, en outre, fixer des règles d'ordre technique relatives aux données de référence.

4. Analyse des impacts des dispositions envisagées

4.1 Impacts économiques et sociaux

La diffusion et la réutilisation des données de référence participe, selon le groupement français de l'industrie de l'information (GFII) de la création d' *« un écosystème économique innovant, associant producteurs, diffuseurs et agrégateurs d'informations, laboratoires de recherche, professionnels de la dématérialisation, start-up et nouveaux acteurs de l'économie numérique. »*

La liste des données de référence qui est envisagée correspond aux bases de données dont la meilleure diffusion est susceptible d'avoir le plus de bénéfices pour le développement économique, comme l'ont souligné certains acteurs économiques (notamment le GFII)[21].

Ces mêmes données de référence bénéficient, comme mentionné précédemment, également à l'amélioration de l'action publique. Cela aura des effets directs sur l'usager de l'administration en termes de simplification de ses démarches administratives. A cet égard, les données de référence viendront s'articuler avec le dispositif d'échange d'informations au bénéfice de l'usager prévu par l'article L.114-8 du code des relations entre le public et l'administration. En effet, en fonction des domaines et procédures concernés les données de référence viendront alimenter les échanges d'informations ou de données. Outre les avancées en termes de simplification mentionnées plus haut, les dispositions de l'article 5 pourront avoir pour l'usager des effets encore plus directs. L'utilisation d'un même référentiel d'adresses permettra notamment une meilleure efficacité et une meilleure coordination de l'intervention des services d'urgence ou de secours, par exemple dans le cas de la Base Adresse Nationale.

[21] http://www.gfii.fr/uploads/docs/GFII_Donneespivots.pdf

Le décret qui dressera la liste des données de référence pourra être mis à jour afin de pouvoir être en adéquation avec les attentes des utilisateurs actuels ou potentiels des données de référence.

4.2 Impact sur les administrations de l'État et sur les collectivités territoriales

Pour ce qui concerne l'impact sur les autorités administratives responsables ou participant à la production de ces données de référence, il convient de souligner que la mise en œuvre du service public de la donnée ne contraint pas les administrations à produire de données nouvelles. Toutefois, celles-ci devront notamment s'engager sur un niveau de qualité, un degré de disponibilité et respecter certaines dispositions techniques qui seront définies par décret en Conseil d'État.

Ce décret fixera également les conditions de participation des collectivités territoriales, qui ont par exemple un rôle dans la constitution et la mise en œuvre de la Base Adresse Nationale. L'objet du service public de la donnée n'est pas d'obliger les collectivités territoriales à produire de nouvelles données, mais simplement d'améliorer la qualité des données qu'elles transmettent déjà à l'État en vertu d'obligations légales ou réglementaires (telles que celles prévues par le décret n° 94-1112 du 19 décembre 1994 pour la transmission à la DGFiP par les communes de plus de 2000 habitants des créations ou modifications d'adresses). C'est donc seulement dans leur fonction de production primaire des données de référence que les collectivités territoriales sont susceptibles de voir leurs obligations renforcées par le présent article, et non dans une fonction de mise à disposition ou de diffusion de ces données.

En conséquence, la participation des collectivités territoriales au service public de la donnée n'est pas accompagnée d'une compensation. En effet, dans la mesure où aucune d'elles ne sera tenue de produire des données nouvelles, cette participation ne pourrait être analysée ni comme un transfert de compétence donnant lieu à une compensation intégrale, ni comme une extension de compétence au sens de l'article 72-2 de la Constitution. Le présent article ne fait qu'aménager les modalités d'exercice de leurs compétences actuelles de production de données, sous la forme de l'approfondissement d'une compétence au sens de la jurisprudence du conseil constitutionnel[22].

5. Consultations menées

Le Conseil national d'évaluation des normes et la Commission d'accès aux documents administratifs ont été consultés.

6. Textes d'application et Outre-mer

Un décret en Conseil d'État fixera les modalités d'application du présent article.

---

[22] Décision n° 2010-56 QPC du 18 octobre 2010, Département du Val-de-Marne [Mesure d'accompagnement social personnalisé - MASP]

Un décret fixera la liste des données de référence et désignera les administrations responsables de leur production et de leur publication.

L'article 46 du projet de loi rend l'article 9 applicable en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

Section 3
Données d'intérêt général

Article 10
Ouverture des données par défaut dans les contrats de délégation de service public

1. État des lieux

La loi du 8 février 1995 relative aux marchés publics et délégations de service public[23], dispose que le délégataire d'un service public remet, chaque année, un rapport à l'autorité délégante, dit « rapport annuel du délégataire ». Ce rapport, dont le contenu a été précisé par un décret du 14 mars 2005[24], comprend notamment les *« comptes retraçant la totalité des opérations afférentes à l'exécution de la délégation de service public et une analyse de la qualité de service »*[25]. Si certaines collectivités mettent volontairement en ligne les rapports annuels, une telle démarche n'a aujourd'hui rien de systématique[26].

Par ailleurs, l'obligation de publication concerne des données relatives au contrat, mais ne couvre pas l'ensemble beaucoup plus vaste des données produites dans le cadre de l'exécution de la délégation du service public (DSP). En effet, l'exploitation d'une DSP donne aujourd'hui lieu à la production d'un volume croissant de données. Dans le domaine de l'eau par exemple, l'organisme chargé du service constitue des bases de données sur les consommations des ménages et des entreprises, sur les opérations d'entretien du réseau ou sur les fuites. Pour des services publics de vélopartage et d'autopartage, ce sont des données sur les déplacements, les durées d'utilisation ou encore l'usure du parc qui sont générées.

Les données des contrats de DSP, qu'il s'agisse des données relatives au contrat lui-même ou des données générées durant l'exploitation du service public, ne sont donc, dans le cas général, pas accessibles en ligne.

---

[23] Loi n° 95-127 du 8 février 1995 relative aux marchés publics et délégations de service public.
[24] Décret n° 2005-236 du 14 mars 2005 relatif au rapport annuel du délégataire de service public local et modifiant le code général des collectivités territoriales
[25] Article L. 1411-3 du code général des collectivités territoriales.
[26] La loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République (« loi NOTRe »), n'impose pas la publicité de ce rapport : en effet, le principe d'ouverture des données publiques par défaut prévu par son article 106 ne s'étend pas aux informations « *produites ou reçues dans l'exercice d'une mission de service public industriel et commercial* », ce qui est le cas des rapports annuels du délégataire.

2. Objectifs poursuivis

A l'ère du numérique, la bonne exécution du service public implique d'assurer la disponibilité, la qualité et la diffusion des données associées aux activités de ce service, notamment dans le cadre des DSP. La place et la légitimité des services publics dans la société seront renforcées si ces services deviennent une source abondante de données pour leurs utilisateurs et vis-à-vis des autres activités économiques. Dans le cas des DSP, l'ouverture des données contribue en outre à ce que la collectivité publique puisse jouer de manière effective son rôle d'autorité organisatrice.
L'article proposé permet donc de prévoir une clause d'ouverture des données par défaut dans les contrats de délégation de service public. Cette disposition permet d'appliquer aux concessions des dispositions similaires à la clause type « *open data* » des cahiers des clauses administratives générales (CCAG).

Cette disposition n'est pas applicable aux contrats en cours.

3. Nécessité de légiférer

Il n'existe pas pour les délégations de service public de document de référence analogue aux cahiers des clauses administratives générales (CCAG) des marchés publics. Il est donc nécessaire d'introduire la clause « open data » dans la loi pour que sa diffusion se généralise dans les contrats de l'ensemble des délégataires (État, collectivités locales, établissements publics).

4. Analyse des impacts des dispositions envisagées

La publication des données des contrats des DSP permettra une meilleure information des citoyens et une transparence accrue. Ces données ont, de plus, une valeur importante pour la collectivité publique, car elles l'aident à faire évoluer l'organisation du service et à conduire ses politiques. Il est toutefois prévu que la personne morale de droit public pourra exempter le délégataire des obligations prévues au premier alinéa par une décision motivée et rendue publique.

La publication des données par les délégantes impliquera une charge de travail pour ces dernières, qui restera néanmoins modérée (à l'instar des charges induites pour les administrations par l'article 3 du présent projet de loi).

La communication des données d'exploitation des entreprises aux autorités délégantes pourra nécessiter l'adaptation de leur système d'information. Les coûts devraient néanmoins être limités et ponctuels. Par ailleurs, afin de renforcer la prévisibilité de la clause « *open data* », les parties pourraient y faire figurer une liste indicative des types de données concernées.

Impact sur les collectivités territoriales

Le présent article s'appliquera aux collectivités territoriales ayant recours à des délégations de service public, dans la mesure où il modifie l'article L. 1411-3 du code général des collectivités territoriales.

Cependant il ne crée pas en lui-même d'obligation ou de charge nouvelle pour les collectivités territoriales : l'obligation introduite porte sur le délégataire, et ouvre à l'autorité délégante une simple faculté d'exploiter les données fournies et de les publier.

5. Consultations menées

Le Conseil national d'évaluation des normes et la Commission d'accès aux documents administratifs ont été consultés.

6. Outre-mer

L'article 46 du projet de loi rend le I et le III de l'article 10 applicables en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

L'article 48 (II) modifie en conséquence l'article 41-1 de la loi n° 93-122 du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques.

Les dispositions du II de l'article 10 n'ont pas fait l'objet d'une extension d'application en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les terres australes et antarctiques françaises dans la mesure où elles concernent des dispositions du code général des collectivités territoriales qui ne sont pas applicables dans ces collectivités.

Article 11
Ouverture des données dans les conventions de subventions

1. État des lieux

L'article 9-1 de la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations définit les subventions comme « *les contributions facultatives de toute nature, valorisées dans l'acte d'attribution, décidées par les autorités administratives et les organismes chargés de la gestion d'un service public industriel et commercial, justifiées par un intérêt général et destinées à la réalisation d'une action ou d'un projet d'investissement, à la contribution au développement d'activités ou au financement global de l'activité de l'organisme de droit privé bénéficiaire* ». La loi ajoute que « *ces actions, projets ou activités sont initiés, définis et mis en œuvre par les organismes de droit privé bénéficiaires* », ce qui les distingue des missions de service public, dont le contenu est défini par la collectivité publique. L'activité subventionnée a, en revanche, ceci de commun avec la mission de service public qu'elle poursuit un but d'intérêt général.

La loi impose que toute subvention d'un montant annuel supérieur à 23 000 euros[27] donne lieu à la conclusion d'un contrat, qui détermine l'objet, le montant, les modalités de versement et les conditions d'utilisation de la subvention attribuée.

Des dispositions sur la transparence financière des subventions existent depuis la loi du 12 avril 2000, qui a notamment prévu que le budget et les comptes de tout organisme de droit privé ayant reçu une subvention étaient communicables à toute personne qui en faisait la demande.

La publication de ces informations n'est cependant pas organisée, sauf dans des domaines particuliers tels que les aides à la presse, la politique agricole commune (PAC) ou l'aide publique au développement.

2. Objectifs poursuivis

L'objectif de la disposition est d'introduire une obligation de publication des données essentielles des contrats de subventions.

L'ouverture des données des subventions présente un enjeu indéniable de transparence démocratique : la subvention relève d'une décision discrétionnaire de la puissance publique et procure un avantage financier direct à son bénéficiaire.

L'article prévoit que la publication des données essentielles des subventions donnant lieu à un contrat est assurée sur le site internet de la collectivité publique qui les verse ; un site national pourrait agréger ces informations.

---

[27] Montant fixé par l'article 1 du décret n° 2001-495 du 6 juin 2001 pris pour l'application de l'article 10 de la loi n° 2000-321 du 12 avril 2000 et relatif à la transparence financière des aides octroyées par les personnes publiques.

3. Nécessité de légiférer

En raison du grand nombre et de la diversité des autorités administratives attribuant des subventions, une mesure législative est nécessaire pour assurer une transparence effective des données des subventions.

4. Analyse des impacts des dispositions envisagées

Concernant la publication des données essentielles des contrats de subventions, la disposition n'entraîne pas de charge de travail particulière pour les organismes subventionnés, puisqu'ils transmettent déjà les informations concernées à leurs financeurs.

Impact sur les collectivités territoriales

Les impacts mentionnés ci-dessus s'appliqueront similairement aux collectivités territoriales attribuant des subventions. Cette charge devrait notamment rester limitée puisqu'elle se limite aux données essentielles de la convention de subvention et qu'elle ne couvre que les subventions d'un montant inférieur à 23 000 € (selon le seuil réglementaire actuellement en vigueur).

5. Consultations menées

Le Conseil national d'évaluation des normes et la Commission d'accès aux documents administratifs ont été consultés.

6. Textes d'application et Outre-mer

Les conditions d'accessibilité visées au présent article seront fixées par voie réglementaire.

L'article 46 du projet de loi rend le présent article applicable en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

L'article 48 (III) modifie en conséquence l'article 41 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

Article 12
Transmission à la statistique publique sous forme électronique d'informations présentes dans certaines bases de données d'organismes privés dans le but exclusif de réaliser des enquêtes statistiques

1. État des lieux

Les statistiques publiques sont aujourd'hui produites soit à partir d'enquêtes statistiques dont la liste est arrêtée chaque année par le ministre chargé de l'économie, soit à partir de fichiers administratifs auxquels la statistique publique peut avoir accès dans le cadre défini par l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière statistique et l'article 17 bis (1) du règlement européen 223/2009 amendé par le règlement 2015/759 du 29 avril 2015. La réalisation des enquêtes auprès des particuliers ou des personnes morales fait intervenir le cas échéant un nombre important d'enquêteurs employés par la statistique publique, comme par exemple pour l'enquête emploi ou l'indice des prix à la consommation.

La statistique publique dispose de prérogatives contraignantes pour que les personnes privées lui communiquent des données dans le cadre de ses missions : la loi du 7 juin 1951 prévoit pour des enquêtes importantes une obligation de réponse à la charge des personnes privées, assortie de sanctions pécuniaires.

Aux termes de la version en vigueur de cette loi, lorsque le ministre arrête le programme annuel d'enquêtes défini sur proposition du Conseil national de l'information statistique (CNIS)[28], il détermine après avis du Comité du Label[29] celles de ces enquêtes qui auront un caractère obligatoire. L'absence de réponse ou la réponse sciemment inexacte à ces enquêtes est punie d'une amende prononcée par le ministre après avis du CNIS réuni en comité du contentieux des enquêtes statistiques obligatoires. Le montant des amendes est à ce jour relativement limité, puisqu'il ne peut dépasser 2 250 euros pour chaque infraction.

2. Objectifs poursuivis

L'objectif de cet article est d'autoriser l'accès de la statistique publique à des informations définies au préalable par la loi qui sont présentes dans des bases de données informatiques gérées par des personnes privées.

L'accès du service statistique public à des informations présentes dans des bases de données ne représente pas un changement de nature de l'obligation statistique : les personnes privées

[28] Le CNIS est défini par la loi comme une instance de concertation entre les producteurs et les utilisateurs de la statistique publique. Il comporte notamment des représentants des partenaires sociaux et des organismes consulaires (chambres de commerce et d'industrie, chambres des métiers et de l'artisanat et chambres d'agriculture).

[29] Le Comité du Label, défini par la loi du 7 juin 1951 est une instance composée d'experts et de représentants des entreprises, de l'administration et des chercheurs qui évaluent la qualité technique des enquêtes et donnent un avis quant au caractère obligatoire ou non d'une enquête demandé par l'entité en charge de la réaliser.

sont déjà tenues de transmettre les informations dont l'utilité a justifié l'inscription dans le programme annuel d'enquêtes obligatoires. Il s'agit d'une modalité nouvelle de mise en œuvre de cette obligation, le service statistique public accédant, au terme d'une étude faisabilité et d'opportunité rendue publique, après concertation sur les modalités techniques avec les personnes privées concernées ou leurs représentants au sein de fédérations professionnelles, et après avis du CNIS, à certains éléments de leurs bases de données au lieu de leur demander d'en extraire les informations nécessaires.

Cet accès ne sera envisagé que lorsqu'il permettra des économies pour les personnes privées ou pour la statistique publique, ou une amélioration de la qualité de la statistique publique par rapport aux modes traditionnels de collecte.

Un exemple de l'intérêt de produire une statistique publique à partir de données privées peut être donné pour le calcul de l'inflation. Aujourd'hui, l'Insee assoit ce calcul en grande partie sur des relevés de prix réalisés dans les différents points de vente par un réseau d'enquêteurs. Une partie de ces relevés (environ 20%) pourrait être remplacée par les prix enregistrés lors du passage en caisse des clients dans la grande consommation (« données de caisse »). Cette opération est réalisable (elle fait l'objet d'une expérimentation depuis plusieurs années), et elle rendrait le calcul de l'inflation moins coûteux et la mesure de l'inflation plus précise. Cependant elle requiert deux garanties : pour l'Insee, que la transmission des données de caisse soit pérenne ; pour les enseignes de grande distribution, que les données transmises servent exclusivement au calcul de l'inflation et à aucun autre usage, y compris statistique (comme la réalisation d'études).

Le secret statistique, en vertu duquel les agents du service statistique public sont astreints au secret professionnel sous les sanctions prévues à l'article 226-13 du code pénal, est applicable aux informations obtenues par l'accès aux bases de données des personnes privées. Deux garanties complémentaires, adaptées à ce nouveau mode de collecte, seront instaurées :

- La limitation de l'accès et de la réutilisation aux données nécessaires à l'enquête : les données collectées ne doivent servir que pour répondre aux besoins de l'enquête, préalablement définis dans le projet d'enquête ayant reçu le visa ministériel prévu par l'article 2 de la loi du 7 juin 1951.
- La sécurité des données : les conditions techniques de la collecte des données devront être définies en accord avec la personne privée, de manière à en garantir la confidentialité et à ne pas affecter la bonne marche de l'entreprise.

Par ailleurs, la problématique des conséquences attachées au non-respect d'une obligation de communication des données doit être traitée. Les sanctions définies par l'article 7 de la loi du 7 juin 1951 pour le refus de répondre à une enquête seraient applicables au refus de laisser le service statistique accéder à des données. La faiblesse de leur montant n'assure cependant pas leur caractère dissuasif et le rend sans rapport avec le surcoût induit sur le système statistique public par un non-respect de l'obligation. Le II de l'article 7 bis instaure donc un régime de sanction spécifique avec des montants maximaux plus élevés.

3. Nécessité de légiférer

L'expérience de l'INSEE sur les données de caisse nécessaires à l'établissement de l'indice des prix à la consommation montre que la coopération volontaire des entreprises n'est pas

suffisante. En effet, il suffit qu'un acteur économique important refuse de coopérer pour que la valeur statistique de l'indice soit remise en cause.

Les dispositions actuelles du second alinéa de l'article 3 de la loi du 7 juin 1951, issues de la loi du 22 mars 2012, ne comportent pas de garantie suffisante pour les personnes privées concernées. Une nouvelle mesure législative est donc nécessaire pour renforcer ces garanties.

4. Analyse des impacts des dispositions envisagées

4.1 Impacts pour les administrations

Les dispositions proposées permettront d'engendrer des économies pour la statistique publique : un accès organisé aux bases de données permet de simplifier les modalités d'interrogation des personnes privées et de réduire le coût de la production des enquêtes statistiques.

L'accès à ces données peut améliorer la qualité des statistiques produites, par l'utilisation de sources plus riches et plus exhaustives. Il peut aussi rendre possible une production régulière de statistiques dont la fréquence est aujourd'hui réduite en raison de leur coût de production élevé. Il pourrait en être ainsi de la population présente sur un territoire, qui permet de dimensionner les infrastructures et les installations de secours, et dont la mesure pourrait reposer sur des données de téléphonie mobile.

4.2 Impacts pour les entreprises

L'accès organisé aux bases de données peut être source de moindres coûts pour les personnes privées, en particulier pour les entreprises. En effet, la réponse aux enquêtes implique la mobilisation de ressources humaines et s'ajoute à d'autres obligations administratives. Ce mode de collecte peut nécessiter certains coûts d'adaptation du système informatique et d'opération de gestion pour permettre la transmission des données à la statistique publique, mais une fois cet effort consenti, il devrait représenter une charge inférieure à celle représentée aujourd'hui par la réponse aux enquêtes.

Par ailleurs cette transmission n'aura pas d'impact économique sur les entreprises : elle devra se faire dans des conditions où l'utilisation des données par la statistique publique ne porte aucune atteinte à leur valeur économique.

5. Textes d'application et Outre-mer

Les conditions de réalisation des enquêtes visées au présent article seront fixées par voie réglementaire.

L'article 46 du projet de loi rend le présent article applicable à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

Section 4
Gouvernance

Articles 13 à 16
Gouvernance

1. **État des lieux**

La Commission d'accès aux documents administratifs (CADA) est une autorité administrative indépendante créée par la loi du 17 juillet 1978. Son rôle principal est de rendre des avis sur les refus de communication des documents administratifs, pour lesquels sa saisine est obligatoire avant tout recours contentieux. Elle peut également être saisie et rendre des avis sur les décisions défavorables des administrations en matière de réutilisation des informations publiques. Elle peut conseiller les administrations sur le caractère communicable d'un document, et peut être consultée par le gouvernement ou proposer des modifications sur des textes législatifs ou réglementaires. Elle assure une fonction de suivi et de soutien auprès des 1800 personnes responsables de l'accès aux documents administratifs (PRADA).

La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante créée par la loi du 6 janvier 1978 afin de protéger les données personnelles des individus. Elle a pour missions principales d'informer sur leurs droits et obligations les individus et les responsables de traitements automatisés de données personnelles et d'autoriser certains traitements de données. Elle joue également un rôle de conseil auprès des acteurs privés ou publics en matière de données personnelles.

Il existe aujourd'hui des recoupements entre les missions de la CNIL et de la CADA, qui représentent une part significative de leur activité. La CADA est ainsi amenée à se prononcer sur la publication ou la réutilisation de fichiers de grande taille comportant des données personnelles, parfois sensibles (données individuelles de santé par exemple). La CNIL de son côté est amenée à se prononcer sur des traitements automatisées de données personnelles utilisant des informations issues de documents administratifs.

Ces recoupements représentent une activité croissante pour la CNIL comme pour la CADA et il est prévisible qu'ils vont croître à l'avenir. La section 1 du chapitre 1er du titre Ier du présent projet de loi augmente fortement les obligations de publication des données publiques et le droit de les réutiliser, notamment en ce qui concerne les informations publiques comportant des données personnelles ; corrélativement, ils prévoient de confier à la CADA de nouvelles missions liées à la mise en œuvre de ces dispositions (émettre des avis sur les refus de publication de documents administratifs, mener une politique active pour constater les manquements aux obligations de publication et inciter les administrations à y remédier).

L'article 29 du présent projet de loi prévoit également d'accroître les missions de la CNIL.

Ces recoupements croissants entre l'activité de la CNIL et de la CADA nécessitent une coordination étroite. Or celle-ci apparaît aujourd'hui insuffisante : elle repose principalement sur la présence dans le collège de la CADA d'un membre désigné par le président de la CNIL, sans qu'une disposition symétrique soit prévue pour le collège de la CNIL. Aucune autre disposition juridique n'est prévue pour garantir la coordination des deux autorités.

2. Objectifs poursuivis

L'objectif de la réforme est de garantir une coordination accrue entre la CNIL et la CADA, permettant une convergence de leur doctrine en ce qui concerne la publication et la réutilisation des données personnelles issues des administrations publiques.

Les articles 13 à 16 du présent projet de loi cherchent à atteindre cet objectif par deux moyens complémentaires :

- Garantir une représentation symétrique de la CNIL au sein du collège de la CADA et de la CADA au sein du collège de la CNIL : les articles 13 et 15 prévoient que le président de la CNIL ou son représentant siégera désormais au collège de la CADA et que le président de la CADA ou son représentant siégera désormais au collège de la CNIL.
- Permettre aux deux autorités de siéger conjointement pour traiter des sujets qui les concernent toutes les deux : les articles 14 et 16 ouvrent ainsi la possibilité aux deux autorités de se réunir dans un collège unique, à l'initiative conjointe de leurs présidents, lorsqu'un sujet d'intérêt commun le justifie.

3. Nécessité de légiférer

Dans la mesure où la composition des deux autorités administratives indépendantes est fixée par la loi (article 13 de la loi du 6 janvier 1978 pour la CNIL, et article 23 de la loi du 17 juillet 1978 pour la CADA), une modification législative est indispensable pour introduire la participation du président de chacune d'entre elles au collège de l'autre autorité.

4. Analyse des impacts des dispositions envisagées

Les présents articles mettent en place des procédures régulières pour garantir la coordination et la concertation entre la CNIL et la CADA. Ils permettront ainsi la constitution d'une doctrine partagée entre les deux autorités et un traitement plus efficace des demandes relatives aux sujets qui leur sont communs.

Ce rapprochement sera bénéfique en lui-même, et constituera également un contexte favorable à une éventuelle fusion de la CNIL et de la CADA, si elle était envisagée à moyen terme.

5. Consultations menées

La Commission d'accès aux documents administratifs et la Commission nationale de l'informatique et des libertés ont été consultées.

6. Outre-mer

L'article 46 du projet de loi rend les présents articles applicables en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

Chapitre II

Economie du savoir

Article 17
Accès aux travaux de la recherche financée par des fonds publics

Le présent article du projet de loi appréhende les travaux de recherche financés sur fonds publics et a pour objet d'ouvrir de nouvelles possibilités de diffusion et d'accès aux produits de la recherche scientifique.

1. État des lieux

Le passage au numérique a fondamentalement changé l'équilibre entre éditeurs, auteurs, communautés et institutions scientifiques. En effet, la diffusion numérique des revues s'est accompagnée :

- d'une hausse des prix des abonnements qui a contraint les bibliothèques des établissements d'enseignement supérieur et de recherche à réorienter leurs acquisitions, en procédant à des désabonnements et en diminuant leurs achats de livres. En France, entre 2002 et 2014, les dépenses de documentation électronique destinées aux laboratoires ont augmenté de 450 %[30],
- de la concentration du marché autour de grands groupes éditoriaux proposant des bouquets de revues incontournables pour les chercheurs, tendant à évincer les éditeurs de taille et de bassin linguistique plus limités,
- du passage d'un modèle de vente pérenne à celui d'abonnements à des flux, sans possibilité de conservation de certaines publications pour les institutions académiques.

Le développement du numérique dans la diffusion scientifique conduit à cette situation paradoxale où un développement rapide du nombre de revues créées et d'articles publiés chaque année s'accompagne d'un appauvrissement de la diversité et de la profondeur des publications effectivement accessibles pour les chercheurs et à un renchérissement global des dépenses d'acquisitions.

[30] Enquête de l'Association des directeurs de bibliothèques universitaires ADBU sur les budgets d'acquisition des BU : http://adbu.fr/wp-content/uploads/2014/03/Enqu%C3%AAte_ADBU_2014.pdf

Parallèlement, ces évolutions ont également des effets importants sur les données scientifiques que produisent les chercheurs et qui sont au fondement des raisonnements qu'ils développent dans leurs écrits. Il peut s'agir de données d'observation, capturées en temps réel, comme en neuro-imagerie, en photographie astronomique ou dans le cadre d'enquête ; de données expérimentales obtenues à partir d'équipements de laboratoire, telles des chromatogrammes ; de données computationnelles, générées par des modèles informatiques, par exemple en météorologie ou en économie ; ou encore de données dérivées, issues du traitement ou de la combinaison de données brutes ou de petits jeux de données, comme dans le cas de bases de données génétiques, de résultats de fouilles de texte, ou de collections d'écrits ou d'archives historiques[31].

Grâce au numérique, ces données se développent rapidement, en nombre et en sophistication, et leur diffusion joue un rôle toujours plus important dans toutes les disciplines. En y accédant librement, les collègues chercheurs peuvent en effet les explorer, les visualiser et les comparer, et effectuer leurs propres analyses, afin de valider ou d'infirmer les conclusions qu'ont tirées les auteurs. Il est devenu courant, sinon impératif pour les chercheurs de rendre les données accessibles aux côtés des écrits, sur la plate-forme de l'éditeur, sous la forme de fichiers numériques ou par l'intermédiaire de liens hypertexte, en plus d'intégrer certaines des données directement au texte de la publication.

La difficulté réside dans le fait que les éditeurs, en tant qu'opérateurs du service de mise à disposition, tendent, dans les contrats de cession portant sur l'écrit, à demander des licences toujours plus étendues sur l'exploitation de ces données, ce qui n'est pas sans poser de risques sur leur libre circulation, essentielle au bon fonctionnement de la recherche.

La situation est particulièrement problématique pour l'accès aux productions de la recherche publique, dont la plus grande partie des coûts sont pris en charge par la puissance publique. Dans le cas de la publication d'articles, les auteurs-chercheurs ne sont qu'exceptionnellement rémunérés par les éditeurs, sauf dans certains domaines comme le droit. De même, le travail d'évaluation par les pairs est en général réalisé de manière gratuite par les chercheurs[32].

2. Objectifs poursuivis

Compte tenu des effets ambivalents de ce contexte sur la circulation scientifique, il importe de favoriser une diffusion étendue des résultats de la recherche, en levant les entraves à leur

[31] La définition suivante pourrait être proposée : « les données de la recherche sont l'ensemble des données factuelles issues d'observations, d'enquêtes, de corpus, d'archives, d'expériences ou d'analyses computationnelles, enregistrées sous tout format et sur tout support, dans une forme brute ou après avoir été traitées ou combinées, et sur lesquelles se fondent les raisonnements du chercheur et qui sont jugées nécessaires à la validation des résultats de la recherche ».

[32] Dans le secteur particulier de l'édition de sciences humaines et sociales français, le travail de secrétariat de rédaction est assuré principalement par des salariés publics, tandis que les éditeurs se chargent de l'impression et de la diffusion, représentant environ 25 % des coûts de publication (enquête Bibliothèque scientifique numérique : Odile Contat et Anne-Solweig Gremillet, « Publier : à quel prix ? Étude sur la structuration des coûts de publication pour les revues françaises en SHS », Revue française des sciences de l'information et de la communication [En ligne], 7 | 2015, mis en ligne le 13 octobre 2015, consulté le 19 novembre 2015. URL : http://rfsic.revues.org/1716).

circulation et en recherchant un nouvel équilibre plus juste entre les intérêts du monde de la recherche et du secteur de l'édition à l'heure du numérique et de la société de la connaissance.

Il s'agit en même temps de mieux valoriser l'investissement public dans la recherche scientifique, en garantissant la possibilité pour les chercheurs dont les travaux sont majoritairement financés par des fonds publics de rendre rapidement leurs travaux disponibles à l'ensemble de la communauté scientifique. A la faculté ainsi ouverte à chaque chercheur de mettre à disposition le fruit de ses travaux répond ainsi la faculté nouvelle pour ses collègues d'accéder librement à l'état le plus avancé de la science dans leurs domaines d'activité.

Il s'agit enfin de reconnaître que les données de la recherche produites par ces chercheurs sont des données d'intérêt public dont la vocation même est de pouvoir circuler dès lors qu'elles ont été rendues publiques. Nul ne doit pouvoir priver autrui de leur usage. Cet objectif rencontre celui de la transparence et de l'intégrité de la recherche, valeurs auxquelles la communauté scientifique est attachée. Il s'agit en même temps de mettre fin aux formes de capitalisation sur les données qui se développent dans le domaine de l'édition scientifique, dès lors que des données accompagnent des écrits qui, pourtant, sont seuls protégés, par principe et sauf nature particulière des données, par des droits de propriété littéraire et artistique.

Deux limites légitimes doivent cependant être posées à ce principe :

a) Il s'agit d'abord d'exclure du périmètre des données concernées les données qui, du fait de leur nature ou du contexte dans lequel elles ont été produites, sont soumises à des droits particuliers, qu'ils soient d'origine contractuelle ou légale. Il faut notamment évoquer à cet égard la protection due au respect de la vie privée, aux données à caractère personnel, et à la propriété intellectuelle. Ces données mises à l'écart, les autres données ont vocation à pouvoir être librement réutilisées ;

b) Il s'agit ensuite de subordonner l'entrée des données dans un régime de libre réutilisation à leur publication effective, afin de préserver les données confidentielles en vertu d'un contrat de collaboration, ou au titre de secrets protégés par la loi, comme le secret professionnel ou le secret défense. Ainsi, une fois que les chercheurs ou leurs établissements ont décidé de rendre leurs données publiques, aucun obstacle ne doit pouvoir entraver leur libre réutilisation.

Une étude récente a ainsi mis en évidence l'effet bénéfique de l'ouverture d'une publication en sciences humaines et sociales sur son audience. Elle montre que l'accès gratuit à une publication auparavant payante provoque un "effet rebond" propice à sa diffusion, et que plus l'accès gratuit est précoce, plus l'audience totale de la publication est importante [33]. De même une étude anglaise récente parvient à une estimation tendant à montrer que les bénéfices d'une politique de diffusion et de réutilisation des données de la recherche pourraient être quatre fois supérieurs à son coût, en tenant compte des économies réalisées[34].

[33] Rapport de l'Institut des politiques publique IPP n°11, juillet 2015 : *Les revues de sciences humaines et sociales en France : libre accès et audience* : http://www.ipp.eu/wp-content/uploads/2015/07/revues-shs-rapport-IPP-juillet2015.pdf.

[34] Identifying benefits arising from the curation and open sharing of research data produced by UK Higher Education and research Institutes, 2008 : http://repository.jisc.ac.uk/279/2/JISC_data_sharing_finalreport.pdf, page 72.

La visibilité et la compétitivité de la recherche française sur la scène mondiale sont des enjeux primordiaux, dans un contexte international de plus en plus concurrentiel[35]. A cet égard, l'accès ouvert aux publications et aux données scientifiques françaises contribue au rayonnement de la recherche française, comme à celui de la francophonie. La diffusion du savoir constitue aussi un facteur de développement pour les pays émergents, dont les institutions académiques ne sont pas toujours en mesure de s'acquitter des coûts de la documentation scientifique. A l'échelle nationale, l'accès ouvert aux publications et aux données de la recherche participe d'une démarche d'innovation ouverte, qui permet à chacun de se saisir librement des résultats de la science.

La diffusion libre des résultats de la recherche relève également de la diffusion générale des connaissances dans la société du savoir qui s'ouvre avec la révolution numérique[36]. Les nouveaux modes d'évaluation de la recherche qui émergent (*altmetrics*) traduisent en parallèle cette nouvelle approche : il ne s'agit plus seulement de s'intéresser à la circulation des résultats de recherche à l'intérieur des communautés scientifiques mais aussi à la façon dont ils sont reçus par la société tout entière. L'accélération de la mise en accès ouvert des productions scientifiques ne peut que favoriser cette circulation auprès d'un public plus large, y compris auprès des publics empêchés, en favorisant l'adaptation des ressources libres à leurs besoins.

3. Options possibles et nécessité de légiférer

3.1 Option possible en dehors de l'intervention de règles nouvelles :

La "voie dorée" (ou "*Open Access Gold*") constitue une possibilité pour développer l'accès ouvert aux résultats de la recherche à l'ensemble de la communauté des chercheurs et des citoyens. Dans ce modèle, aussi appelé "auteur-payeur", les coûts de "libération" de l'article (*Article processing charge* - APC) sont payés dès sa parution par l'institution à laquelle est rattaché l'auteur. L'avantage de ce processus est que l'article ainsi publié est immédiatement accessible à tous sans délai, et que les risques de perte de chiffre d'affaires pour les éditeurs sont parfaitement maîtrisés.

Pour une grande majorité de chercheurs en France, ce modèle, en pleine expansion dans les politiques éditoriales, reste étranger à leur conception de l'édition scientifique : parmi les directeurs d'unités publiantes du CNRS, 83 % de ceux qui n'ont jamais payé pour faire éditer un article en accès ouvert déclarent qu'ils n'envisagent pas de le faire[37].

En outre, des interrogations se font jour sur la soutenabilité financière de ce modèle à long terme. A titre d'exemple, si on fait l'hypothèse extrême qu'à terme tous ses articles sont publiés en accès ouvert sur la base d'un montant d'APC de 2 200 € par article (moyenne constatée chez l'éditeur *Nature Springer*), le coût de la "voie dorée" généralisée supporté par

[35] *État de l'enseignement supérieur et de la recherche en France*, fiche 46 "Les publications scientifiques de la France", http://publication.enseignementsup-recherche.gouv.fr/eesr/8/EESR8_R_46-les_publications_scientifiques_de_la_france.php#ILL_EESR8_R_46_04a

[36] *Vers les sociétés du Savoir*, rapport de l'Unesco, 2005, page 181.

[37] *Mieux partager l'information scientifique et technique*, CNRS- Direction de l'information scientifique et technique DIST, mars 2015 [Questionnaire adressée aux directeurs des 1250 unités publiantes du CNRS] : http://www.cnrs.fr/dist/z-outils/documents/Enqu%C3%AAte%20DU%20-%20DIST%20mars%202015.pdf.

le CNRS serait six fois plus important que son budget d'abonnements actuel[38]. La publication d'un article dans une revue *gold* exige en outre plus de temps que le dépôt dans une archive institutionnelle telle HAL, ce qui se traduit par des coûts supplémentaires de nature salariale[39].

Enfin, le modèle "auteur-payeur" ne semble pas garantir un facteur d'impact plus important aux revues que les autres modèles de publications en accès ouvert[40]. De manière générale, sa généralisation risquerait d'accroître les inégalités entre établissements, entre disciplines selon leurs tailles et les capacités contributives de leur audience, et pourrait créer des suspicions sur la qualité de la sélection des articles, compte tenu des nouvelles incitations économiques pour les éditeurs de revues. Dans les cas extrêmes des « revues prédatrices »[41] – ces nouvelles revues apparues uniquement pour profiter de l'effet d'aubaine du Gold – il n'y a plus aucune sélection des articles, et y publier n'a donc aucune valeur scientifique : face à leur multiplication, des alertes ont été lancées pour prévenir notamment les jeunes chercheurs qui n'ont pas encore une bonne connaissance du paysage éditorial scientifique.

En ce qui concerne la libre diffusion des données de la recherche, l'absence d'une protection garantie par la loi laisse le champ libre à des formes abusives de capitalisation sur les fruits de la dépense publique par des acteurs privés, en dépit de déclarations de principe contraires exprimées depuis une dizaine d'années[42]. Dans ces conditions, l'introduction de nouvelles règles paraît nécessaire.

Choix des délais maximaux d'embargo :

La mise en place d'embargos est le résultat d'un compromis entre les intérêts de l'éditeur, soucieux de disposer d'un temps d'exploitation économique exclusive de la publication, et les attentes de la communauté de la recherche, attachée à une diffusion libre de la connaissance la plus rapide possible.

Les délais maximaux d'embargo ont été fixés à 6 mois pour les sciences, la technique et la médecine et 12 mois pour les sciences humaines et sociales. Ces durées sont conformes aux délais préconisés par la recommandation précitée de la Commission européenne du 17 juillet 2012.

Ils sont également comparables ou identiques aux délais choisis par les autres pays ayant pris des mesures législatives ou réglementaires en matière de libre accès aux publications scientifiques, tout comme à ceux choisis par les institutions de financement de la recherche nationales et internationales. Ainsi, par exemple : Allemagne (12/12 mois), Argentine (6/6 mois), États-Unis (12/12 mois), Espagne (12/12 mois), Italie (18/24 mois) ; programme cadre

---

[38] *Financer la publication scientifique*, CNRS-DIST, juin 2015 : http://www.cnrs.fr/dist/z-outils/documents/Distinfo2/DISTetude3.pdf

[39] *Counting the cost of Open Access*, London Higher et SPARC Europe, novembre 2014 : http://www.researchconsulting.co.uk/wp-content/uploads/2014/11/Research-Consulting-Counting-the-Costs-of-OA-Final.pdf.

[40] *Proportion of Open Access Peer-Reviewed Papers at the European and Words levels - 2004-2011*, rapport commandé par la Commission européenne, août 2013 : http://www.science-metrix.com/pdf/SM_EC_OA_Availability_2004-2011.pdf.

[41] Cf. « Revues « prédatrices » : un danger pour les chercheurs ! » : http://openarchiv.hypotheses.org/2044

[42] Le principe d'une libre diffusion des données de la recherche est notamment inscrit dans la déclaration de Bruxelles signée en 2007 par les plus grands éditeurs scientifiques mondiaux. http://www.stm-assoc.org/public-affairs/resources/brussels-declaration/

de recherche Horizon 2020 (6/12 mois), Research Council UK (6/12 mois), agences canadiennes (12/12 mois), agences indiennes (6/12 mois).

Parallèlement, les délais d'embargo pratiqués par une grande partie des éditeurs nationaux et internationaux s'étalent aujourd'hui entre 0 et 24 mois, exceptionnellement jusqu'à 48 mois pour certaines revues de sciences humaines et sociales. Il demeure également des éditeurs qui s'opposent à la possibilité d'une rediffusion des publications, même à des fins non commerciales, par les chercheurs.

3.2 Motifs du recours à une nouvelle législation :

Il s'agit d'ouvrir la possibilité d'une diffusion en accès libre des travaux scientifiques financés sur fonds publics, au terme d'une durée dite « d'embargo » préservant les droits exclusifs des éditeurs. Il s'agit en même temps de sécuriser juridiquement des pratiques existantes dans la communauté scientifique et bien tolérées par les éditeurs. La création de ce nouveau droit pour les auteurs des travaux nécessite l'intervention du législateur, afin qu'il s'impose dans l'ensemble des contrats d'édition à venir. Cette disposition crée un nouveau droit pour l'auteur de la publication et promeut un nouvel équilibre dans la relation entre un chercheur et son éditeur.

La mesure proposée suit les recommandations du 17 juillet 2012 de la Commission européenne relatives à l'accès et la préservation des informations scientifiques[43], qui appellent notamment à veiller :
- *« à ce que les publications issues de la recherche financée par des fonds publics soient librement accessibles dans les meilleurs délais, de préférence immédiatement et, dans tous les cas, au plus tard six mois après leur date de publication, et au plus tard douze mois pour les publications dans les domaines des sciences sociales et humaines » ;*
- *« à ce que les systèmes d'octroi de licences contribuent, de façon équilibrée, au libre accès aux publications scientifiques issues de la recherche financée par des fonds publics, dans le respect et sans préjudice de la législation applicable en matière de droit d'auteur, et encouragent les chercheurs à conserver leurs droits d'auteur tout en concédant des licences aux éditeurs (...) ».*

La mesure vise également à favoriser et à protéger la libre réutilisation des données de la recherche, à partir du moment où elles sont rendues publiques. Elle suit en cela les lignes directrices du programme-cadre de recherche européen Horizon 2020 (2014-2020), qui encourage la diffusion en « *open access* » de toutes les données nécessaires à la validation des résultats présentés dans les publications. Elle est conforme à l'esprit de la déclaration de Berlin de 2003 sur le libre accès à la connaissance, signée par les plus grands établissements scientifiques mondiaux[44], ainsi qu'à la déclaration de Bruxelles précitée, portée par le secteur de l'édition. Elle répond enfin à une forte demande de la communauté de la recherche, exprimée par plusieurs contributions dans le cadre de la mise en consultation du projet de loi

[43] https://ec.europa.eu/research/science-society/document_library/pdf_06/recommendation-access-and-preservation-scientific-information_fr.pdf
[44] Déclaration de Berlin sur le libre accès à la connaissance en sciences exactes, sciences de la vie, sciences humaines et sociales http://openaccess.mpg.de/Berlin-Declaration
http://openaccess.mpg.de/68042/BerlinDeclaration_wsis_fr.pdf

en ligne, et particulièrement à l'occasion du « GouvCamp » du 16 octobre 2015, qui a rassemblé les principaux représentants de l'informatique scientifique et technique français[45].

Cette libre diffusion et réutilisation des données de la recherche est favorisée de deux manières :

- D'une part, la mesure spécifie que les données de la recherche non protégées issues de travaux financés majoritairement sur fonds publics sont librement réutilisables, à partir du moment où elles ont été rendues publiques, posant ainsi les prémices d'une définition positive du domaine commun de la connaissance.
- D'autre part, la disposition interdit plus généralement à l'éditeur d'un écrit de restreindre la réutilisation de données liées à des travaux financés majoritairement sur fonds publics dans le cadre d'un contrat d'édition.

Ces mesures sont d'ordre public.

4. Analyse des impacts des dispositions envisagées

4.1 Impact pour la puissance publique :

La mise en place de délais d'embargo et la libre réutilisation des données de recherches par les chercheurs autorisent une maîtrise accrue de la puissance publique sur les produits d'une activité de recherche qu'elle a elle-même financée. A l'image de l'évolution constatée dans de nombreux pays, l'adoption par la France de mesures en faveur du libre accès est de nature à favoriser le développement du mouvement de « *l'open access* » et à instaurer une relation plus équilibrée entre les institutions académiques et le secteur de l'édition scientifique à l'échelle nationale, voire européenne et mondiale. Sur le long terme, cette évolution favorise une meilleure régulation des coûts de l'information scientifique et technique, aujourd'hui largement supportés par la puissance publique.

4.2 Impact économique et social :

En augmentant la productivité de la recherche et en démocratisant leur accès, le partage des données de la recherche concourt au développement économique et social. A titre d'exemple, les bénéfices économiques du projet international de séquençage du génome humain INSDC[46], qui repose sur une contribution internationale à une banque ouverte de données, a été estimé à 800 milliards de dollars, s'accompagnant d'une création de 310 000 emplois, pour 3,8 milliards investis par le gouvernement américain[47].

4.3 Impacts sur la recherche :

La mise en accès ouvert de publications et la libre réutilisation des données de la recherche favorise le partage des connaissances et des découvertes, anciennes et récentes, au sein de la communauté scientifique. Elle encourage les collaborations et l'interdisciplinarité, limite la

[45] http://www.republique-numerique.fr/events/gouvcamp-projet-de-loi-numerique
[46] http://www.insdc.org/
[47] https://ec.europa.eu/research/science-society/document_library/pdf_06/era-communication-towards-better-access-to-scientific-information_fr.pdf

duplication des efforts de recherche, contribue à l'amélioration générale de la qualité des travaux. Elle ouvre également la voie à une meilleure prise en compte des attentes de la société civile, favorisant une recherche et une innovation responsables. Elle profite enfin aux entreprises qui cherchent à innover, en particulier aux petites et moyennes entreprises qui n'ont pas les capacités d'investir dans la recherche et développement.

4.4 Impacts sur l'économie de l'édition scientifique :

a) Publications scientifiques

A titre liminaire, il est important de noter que la mesure laisse au chercheur le choix de mettre ses publications en accès ouvert ou de ne pas le faire, laissant aux nouvelles pratiques le temps de se développer librement. Les effets éventuels de la nouvelle législation sur l'économie de l'édition scientifique devraient ainsi être lissés sur plusieurs années[48].

En outre, la mesure assigne un périmètre limité aux publications concernées, qui sont celles issues de la recherche publique financées à 50% sur fonds publics.

En choisissant un seuil de 50 % de part de fonds publics dans le financement pour qualifier les activités de recherche visées par la mesure proposée, le Gouvernement a privilégié un critère simple et quantifiable, répondant à la nécessité de distinguer clairement les activités financées essentiellement sur fonds privés, qui n'ont pas vocation à être concernées. Le critère se laisse naturellement insérer et évaluer dans les conventions passées entre les opérateurs publics de recherche et les entreprises. Cette approche est également celle retenue par l'Allemagne et l'Italie, principaux pays à avoir légiféré sur *l'open access*. La détermination des coûts de financement se fondent sur une analyse en « coût complet », qui intègre notamment les coûts salariaux associés au travail de recherche.

Afin d'évaluer le risque de baisse de chiffre d'affaires associé à la mesure proposée, il s'agit de distinguer l'effet sur les pratiques d'achat d'articles à l'unité de celui sur l'abonnement aux revues, que les éditeurs commercialisent en général par bouquets de quelques dizaines à quelques milliers de revues. Une étude commandée par le diffuseur Cairn.info, plateforme spécialisée dans les revues en sciences humaines et sociales (SHS), indique que la part de vente à l'unité dans son chiffre d'affaires est très limitée, puisqu'elle n'est globalement que de 3,9%, et que de 2,54% (soit 96.000 € en 2014, sur un chiffre d'affaires de 3,77 M€) si on considère uniquement les ventes d'articles effectuées 12 mois après leur parution[49].

Une autre étude, conduite en 2012 aux États-Unis après quelques années d'existence d'une plate-forme d'accès libre en médecine et sous une législation fixant une durée d'embargo d'un

[48] Un article du journal allemand *Tagesspiegel* du 15 juillet 2015 expose qu'à cette date, même après un an et demi d'effectivité du "second droit" de diffusion libre des Allemands, pas plus de 5 à 10 % seulement des articles des chercheurs berlinois sont accessibles en libre accès.
Cf. http://www.tagesspiegel.de/wissen/open-access-freier-forschen-fuer-berliner-unis/12055836.html

[49] L'Open Access et les revues SHS de langue française : Tendances du secteur, évolution de l'environnement réglementaire et perspectives 2018, IDATE / Cairn Info – Octobre 2015 :
http://www.openaccess-shs.info/wp-content/uploads/2015/10/Etude-IDATE-CAIRN-INFO-20151002.pdf

an, tend quant à elle à montrer que la mise en accès ouvert des publications se traduit par un recul limité des accès via les sites des éditeurs[50].

Enfin, le risque de désabonnement à des revues isolées ou à un bouquet de revues, lié directement à la mise en accès libre d'une partie de leur contenu, est plus difficile à évaluer, mais sans doute très faible, dans la mesure où, quelle que soit la durée du délai d'embargo, la possibilité d'accéder aux publications *dès leur parution* demeurera toujours une attente majeure de la part des chercheurs, vis-à-vis de leur établissement ou de leur bibliothèque.

En toute hypothèse, l'expérience allemande nous éclaire : au terme d'une année d'application de la loi, 10 % des chercheurs environ ont fait exercice de leur droit sur leurs nouveaux écrits. Il peut ainsi être raisonnablement estimé que la disposition proposée sera d'impact progressif et mesuré.

b) Données de la recherche

S'agissant des données de la recherche rendues publiques après la publication de la loi, le III de l'article L. 533-4 du code de la recherche créé par le présent projet de loi empêche un éditeur scientifique de limiter leur réutilisation par des tiers, sans préjudice de l'utilisation qu'il pourrait en faire lui-même. La mesure n'est par ailleurs d'aucun effet sur l'exploitation de licences qu'il pourrait détenir sur des données de la recherche rendues publiques dans le passé.

Le commerce de données de la recherche reste un secteur d'activités très peu développé, limité à quelques services spécialisés offrant des services d'analyse et de fouille de données sur des corpus très étendus. L'impact d'une disposition limitant l'exclusivité sur le flux, sans porter atteinte au stock, apparaît limité, au surplus très progressif, à l'échelle microéconomique. A l'échelle macroéconomique, la disposition est au contraire source d'externalités positives importantes à moyen-long terme, ouvrant à tout acteur innovant la possibilité de développer des services à haute valeur ajoutée sur des données accessibles à moindre coût, voire à coût nul.

Focus 1 : Impact économique sur l'édition scientifique institutionnelle en France

L'impact de cette mesure sur les équilibres économiques de l'édition scientifique institutionnelle française, essentiellement constituée d'éditeurs de sciences humaines et sociales, doit être relativisé dans la mesure où la majorité de leur chiffre d'affaires est aujourd'hui constitué de subventions apportées par des établissements ou des laboratoires. Les revues ne représentent en outre, en moyenne, que 18 % de leur production éditoriale, et entre 40 % et 60 % du chiffre global des ventes associées ces revues est réalisé grâce aux publications de l'année, qui demeureront sous embargo au terme de la mesure proposée[51], garantissant que ces acteurs ne devraient être touchés que marginalement.

[50] *Public accessibility of biomedical articles from PubMed Central reduces journal readership retrospective cohort analysis*, Philip M. Davis, avril 2013 : http://www.fasebj.org/content/early/2013/04/03/fj.13-229922.full.pdf+html

[51] Source : *L'édition scientifique institutionnelle en France : état des lieux, matière à réflexions, recommandations*, Jean-Michel Henny, AEDRES, 2015.

Focus 2 : Situation économique de l'édition scientifique mondiale

L'édition scientifique mondiale se caractérise aujourd'hui par une forte concentration, de nature oligopolistique, autour de quelques groupes internationaux. Les 5 premiers éditeurs mondiaux contrôlent ainsi 40 % du marché des revues scientifiques en valeur en 2014. L'information scientifique et technique constitue une activité exceptionnellement rentable, avec un taux de marge opérationnelle moyen de près de 35 % pour les acteurs les plus importants en 2014[52]. Pour cette même année, le premier acteur du secteur, RELX Group (ex-groupe Elsevier) réalise un chiffre d'affaires mondial de 6,1 milliards d'euros (hors expositions) ; Springer Nature, issu de la fusion récente entre Nature Publishing Group, Palgrave Macmillan, Macmillan Education et Springer Science+Business Media réalise pour sa part un chiffre d'affaires de 1,5 milliards d'euros. Leur taux de croissance connaît une progression régulière comprise entre 2 et 4 % par an.

Atteintes aux droits et libertés des chercheurs et éditeurs :

Il n'est pas porté atteinte au droit d'auteur, ni à la liberté de la recherche, la disposition laissant aux auteurs-chercheurs la liberté de ne pas exercer la faculté qui est offerte de mettre leurs écrits à disposition à l'expiration des délais d'embargo, et de ne pas rendre publiques les données issues de leurs travaux.

Il n'est pas porté atteinte aux situations légalement acquises, la disposition ne produisant des effets que sur les contrats d'édition conclus, ou les données rendues publiques postérieurement à l'entrée en vigueur de la loi, et limitant le champ d'application du II du projet d'article L. 533-4 du code de la recherche, qui pose un principe de libre réutilisation sur les données de la recherche, à des données qui ne font pas l'objet d'une protection particulière.

Une atteinte limitée est portée à la liberté contractuelle des auteurs et des éditeurs, le caractère d'ordre public empêchant l'auteur ou son établissement de renoncer au bénéfice du droit qui lui est conféré en ce qui concerne les publications, et de céder à l'éditeur des licences tendant à limiter la réutilisation des données de la recherche. L'atteinte apparaît équilibrée au regard des finalités d'intérêt général poursuivies et conforme à la mission de diffusion des connaissances scientifiques qui est confiée à la recherche publique par l'article 14 de la loi n° 82-610 du 15 juillet 1982 modifiée.

Effectivité :

S'agissant des publications, la disposition sera d'un effet immédiat sur les contrats relevant en cas de litige de la compétence des tribunaux français. Compte tenu des nombreux pays ayant déjà pris des mesures législatives tendant à permettre au chercheur ou à imposer la diffusion

[52] Sources : *L'édition de sciences à l'heure du numérique : dynamique en cours* (2015), DIST-CNRS : http://www.cnrs.fr/dist/z-outils/documents/Distinfo2/Distetude2.pdf ; *Résultats 2014 des grands éditeurs scientifiques : une croissance satisfaisante, des profits records*, DISTinfo14 /mars 2015 : http://www.cnrs.fr/dist/z-outils/documents/Distinfo2/Distinf14.pdf ; rapports financiers annuels des grands éditeurs.

en accès libre des travaux de recherche financés sur fonds publics[53], le risque « d'évasion » des contrats vers des législations moins contraignantes apparaît très limité.

Par ailleurs, il importe de noter que les éditeurs tendent à intégrer les droits nationaux dans les contrats, dans la mesure où l'existence de dispositions nationales interdisant la cession de droits affaiblissent les contrats n'intégrant pas ces dispositions, y compris si ces contrats sont réputés relever d'un droit étranger. Ainsi, les contrats-types des grands éditeurs sont aujourd'hui en mesure de prévoir un périmètre de droits concédés à géométrie variable selon les pays et les institutions de rattachement de l'auteur, qui est interrogé par le contrat-type sur ces points, y compris lorsqu'il s'agit de publications d'agents du gouvernement fédéral américain soumis à un régime de domaine public. Ainsi, la mesure pourra avoir un effet concret sur des contrats régis par un droit étranger. En outre, le risque d'éviction de chercheurs français de revues étrangères paraît par conséquent pouvoir être écarté.

5. Consultations menées

Les principaux représentants de l'édition scientifique opérant en France ont été consultés.

Une consultation large a été menée dans le cadre de la Bibliothèque scientifique numérique (BSN), instance de coordination entre opérateurs de l'enseignement supérieur et de la recherche dans le domaine de l'information scientifique créée en 2009 à l'initiative du ministère de l'enseignement supérieur et de la recherche. BSN fédère l'essentiel des acteurs des universités, écoles et organismes de recherche français. Le ministère de la Culture et de la Communication est associé à ses travaux.

6. Outre-mer

L'article 46 du projet de loi rend l'article 17 applicable en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

L'article 47 (II) modifie en conséquence le code de la recherche pour l'application de l'article L. 533-4 dudit code, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

7. Mesure complémentaire à la loi : plan d'accompagnement des revues en sciences humaines et sociales (SHS) à la transition vers le libre accès

a. Contexte du plan d'accompagnement

Malgré le caractère très limité de l'impact économique immédiat induit par la modification du cadre législatif - lequel n'impose aucune obligation de dépôt aux chercheurs -, que les données chiffrées de l'étude Idate, vues ci-dessus (point 4) permettent de vérifier (a contrario de son scénario « maximaliste » d'un passage généralisé de l'ensemble des revues de SHS en libre accès après un an, aux conséquences plus brutales -), les consultations menées par le MENESR, suivie de la consultation publique sur le projet de loi pour une République

[53] Notamment l'Allemagne, l'Espagne, l'Italie, les Pays-Bas, les Etats-Unis (et spécialement la Californie), le Mexique et l'Argentine.

numérique, ont laissé apparaître néanmoins une crainte de nombreux éditeurs et directeurs de revues de sciences humaines et sociales (SHS), inquiets pour la viabilité de ces dernières en cas d'adoption de la mesure.

Cette inquiétude se nourrit d' une fragilité particulière de l'édition française de revues en SHS, marquée par une diminution tendancielle des abonnements papiers, par le resserrement des budgets d'acquisitions des bibliothèques réorientés vers les plateformes de revues en sciences et médecine très onéreuses, et enfin par le recul de la langue française comme langue scientifique dans le monde.

Si le marché global des SHS (revues et ouvrages scientifiques et grand public) est important – le secteur universitaire de ventes de livres en SHS représente à lui seul 243,4 M€ en 2014[54]-, en revanche la part propre au marché des revues de recherche en SHS est très circonscrite (12 à 13 M€ de chiffre d'affaires en 2009[55]). Une caractéristique du secteur des revues en SHS est d'une part la place des éditeurs publics, avec un apport de moyens en amont (financiers et personnels) relativement stable, et d'autre part les caractéristiques des éditeurs privés – en majorité spécialisés, mais sans la concentration qu'on trouve dans l'édition STM (science, technique, médecine) -[56], bénéficiant d' un soutien public significatif.[57] Néanmoins, le périmètre de leur marché étant restreint (300 abonnés par revue, donnée médiane[58]), l'équilibre économique des revues présente une fragilité particulière.

Cet état de fait s'accompagne d'une évolution de fond qui inquiète également de nombreux chercheurs en SHS : le recul du français comme langue scientifique (avec pour corollaire une baisse des abonnements aux revues réalisés à l'étranger, alors qu'ils réalisent pour certaines d'entre elles près de 50% de leur chiffre d'affaires). Ce phénomène de recul, sensible depuis au moins deux décennies, pose un problème spécifique à des sciences où la fécondité et l'acuité de la recherche dépendent pour une bonne part de la relation à la langue « naturelle ». La réduction de la circulation, accentuée par la surreprésentation de revues en langue anglaise sur les grandes plateformes internationales, produit un effet d'éviction au profit de l'écriture en anglais, qui, dans une majorité de sous-disciplines, peut conduire à un appauvrissement qualitatif. Les politiques de stimulation de la circulation sont donc dans ce domaine des politiques d'aide à la qualité et à la reconnaissance de la production scientifique dans l'univers international de la science.

Ainsi, pour permettre à l'ensemble des acteurs scientifiques de prendre au mieux le tournant important vers le libre accès, et selon la demande du Premier Ministre dans sa lettre du 23 novembre 2015 adressée à la Ministre en charge de l'Enseignement supérieur et de la Recherche, le MENESR propose un plan de transition au libre accès des revues de

[54] Chiffres SNE : http://www.sne.fr/secteur_edit/universitaire-2/

[55] L'édition scientifique française en sciences humaines et sociales, GFII, 2009) : http://www.gfii.fr/uploads/docs/l-edition-scientifique-francaise-en-sciences-sociales-et-humaines.pdf

[56] Parmi une offre d'environ 2000 revues SHS, si l'on considère les 500 titres les plus importants, les groupes français généralistes (Hachette, Editis, La Martinière-Le Seuil, Gallimard-Flammarion) en possèdent moins de 40 ; les éditeurs spécialisés francophones que sont L'Harmattan, Erès, PUF, de Boeck en possèdent moins de 150, le CNRS et les presses universitaires portant le reste des titres avec d'autres acteurs variés : en 2009, le GFII évaluait à 1200 le nombre total d'éditeurs d'une seule revue de SHS, allant d'associations et de sociétés savantes, de petits éditeurs privés spécialisés, à des laboratoires de recherche publics. Sources : études citées dans « Les revues de sciences humaines et sociales (1) : une économie fragile », Jean Pérès, décembre 2014 (Acrimed : http://www.acrimed.org/Les-revues-de-sciences-humaines-et-sociales-1-une-economie-fragile).

[57] Globalement (ouvrages et revues), les « éditeurs privés, au travers du CNL et autres sources d'aides (apports de budgets de publication par les unités de recherche), perçoivent des aides publiques d'un volume de l'ordre de 4 millions d'euros, soit 29% de leurs chiffres d'affaires en édition de recherche. » Source : Etude GFII 2009

[58] « Le nombre d'abonnements payants moyen s'étage entre 150 et 1 200 abonnés avec une médiane de l'ordre de 300 abonnés ». Source : GFII, *L'édition scientifique française en sciences sociales et humaines,* octobre 2009

SHS, en cohérence également avec le juste équilibre entre sciences humaines et sociales et sciences dures, réaffirmé le 19 octobre 2015 par Thierry Mandon lors de son entretien avec Carlos Moedas.

Conjointement à ce plan, le MENESR veillera, avec les acteurs concernés, à fortifier les dispositifs d'observation et d'alerte de l'édition en SHS (mise en place d'un observatoire de l'économie des revues en SHS), avec une attention particulière à l'évolution des politiques des établissements en matière d'incitation des chercheurs en SHS à déposer leurs articles dans des archives ouvertes institutionnelles, et à leur politique d'abonnements. Un tel observatoire est d'autant plus important qu'aucune étude d'envergure sur l'économie des revues en SHS n'a été réalisée depuis les années 2005-2009[59].

b. Principes du plan de transition

L'objectif du plan, qui sera lancé dès 2016, est d'aider les revues qui le souhaiteraient à mettre en accès libre l'intégralité de leurs numéros, soit sans délai soit au terme d'un délai minimal après leur parution pour continuer d'assurer leur viabilité (un an).

Ce mécanisme de diffusion en libre accès, dénommé « barrière mobile », se distingue, par son caractère global et systématique, de l'embargo posé sur les articles, qui bloque durant un temps déterminé (12 mois) le droit de diffusion gratuite accordé à l'auteur par la nouvelle mesure proposée (liberté qu'il exercera ou non, au terme du délai). Un très grand nombre de revues en SHS usent déjà de ce mécanisme, mais avec des délais longs de 2 à 3 ans (47% des revues hébergées sur la plateforme Cairn appliquent ces délais, par exemple), voire très longs, de 4 ans et plus (41% des revues Cairn).

Le plan leur permettrait donc de raccourcir la durée de leurs barrières, avec pour effet immédiat un accroissement et une accélération de la diffusion des résultats de la recherche française (offrant une visibilité accrue à nos universités et organismes de recherche), et plus globalement une meilleure diffusion des savoirs, au bénéfice de l'ensemble de la société.

Périmètre du plan

Le plan, ciblé sur les revues de recherche de haut niveau, s'adresse aux revues :

- françaises, voire francophones,
- sélectionnées sur une base scientifique : dans un premier temps, les revues éligibles sont celles labellisées par le HCERES, soit environ 400 revues. Elles pourraient également, ultérieurement, être sélectionnées par un comité idoine élargi à l'Alliance Athéna, l'OST… ;
- existantes et nouvelles : le plan doit permettre de maintenir les conditions d'une pépinière de revues qui s'adaptent aux évolutions de la connaissance et des thématiques de recherche en SHS, dans un écosystème public et privé qui assure la diversité de l'édition de recherche francophone.

[59] Marc Minon, Ghislaine Chartron : *État des lieux comparatif de l'offre de revues SHS France – Espagne – Italie*, Étude réalisée pour le Ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche, juin 2005 ; Sophie Barluet, *Les revues françaises aujourd'hui : entre désir et dérives, une identité à retrouver,* Rapport de mission pour le Centre national du livre, avril 2006 ; GFII, *L'édition scientifique française en sciences sociales et humaines,* octobre 2009

Modalités du plan

Le plan comprend un dispositif à deux volets favorisant la diffusion des résultats de la recherche française en SHS :

- une aide à l'accélération de la diffusion en libre accès (réduction des barrières mobiles), qui prenne en compte des projets selon des modalités de calcul différentes, s'agissant d'éditeurs publics ou privés,
- par une aide à la traduction en anglais (par exemple de résumés longs), afin de favoriser la diffusion des résultats eux-mêmes, établie en coordination avec les aides déjà existantes du CNRS et du CNL.

Le plan associera, dans un comité d'orientation, les principaux acteurs scientifiques et économiques (en tant qu'acquéreurs d'abonnements par exemple, ou financeurs actuels du soutien aux revues) concernés, qui élaboreront avec les éditeurs et directeurs de revue les modalités d'évolution des modèles de financement permettant d'atteindre l'objectif visé. Sont concernés les organismes et établissements de recherche (CNRS – notamment INSHS -, IRD, EHESS…), la CPU, ainsi que le MCC et le CNL. La BnF et l'ADBU (Association des directeurs de bibliothèques de l'ESR) auront également un rôle important, car les bibliothèques de recherche ont déjà l'expérience de modèles économiques nouveaux, notamment le passage d'un mode de financement en aval, par les acquisitions d'abonnements de revues, à un mode de financement en amont, par l'abonnement à des plateformes proposant des revues en accès libre, mais avec un complément payant de services à valeur ajoutée (modèle « Freemium »). Si cette nouvelle offre reste encore limitée à quelques acteurs (OpenEdition en France, Erudit au Canada), elle tend à se développer et pourrait être soutenue par le plan, notamment auprès de nouveaux acteurs pour maintenir la diversité indispensable de l'offre et des vecteurs de diffusion.

Financement du plan

Le plan proposera une montée graduelle des financements reposant notamment sur des appels à manifestation d'intérêt de la part des éditeurs et directeurs de revues. Une impulsion forte sera donnée par le MENESR, mais l'ensemble des acteurs cités ci-dessus membres de l'écosystème global de la publication scientifique (auteurs – comités de lecture – éditeurs – bibliothèques pour la diffusion des revues imprimées et l'accès aux plateformes de revues), sont concernés.
Dès 2016, l'accompagnement des premières revues volontaires pourra démarrer sur la base d'une enveloppe réservée par le MENESR d'environ 500 K€. Pour la suite, selon la cible visée - barrière mobile ramenée à 12 mois, ou libre accès immédiat, options qui peuvent être panachés en fonction du choix des revus -, l'ordre de grandeur des besoins financiers serait le suivant :

- dans le premier cas (barrière mobile de 12 mois), l'étude Idate permet d'évaluer le coût, pour environ 376 revues de recherche, à 3,15 M€, dont *la moitié* à la charge des établissements, français ou étrangers, via un coût d'abonnement global maintenu à son niveau actuel, voire adapté en une licence nationale (la disponibilité de revues de SHS dans l'ensemble des établissements de l'ESR français favorisant la transdisciplinarité), et *l'autre moitié (1,5 M€)* en accompagnement direct par l'État des revues sélectionnées[60] : ces coûts maximum

[60] Dans l'étude Idate, ce coût est calculé sur l'hypothèse d'une perte de valeur de l'abonnement estimée à 60% en cas de passage global des revues à une barrière mobile de un an. Le maintien du coût d'abonnement actuel à la

seraient toutefois diminués à proportion du nombre effectif de revues soutenues, compte tenu de la sélectivité du plan, qui s'adresserait par ailleurs aux revues quelle que soit leur plateforme de diffusion actuelle ;

- dans le second cas, à savoir le passage au libre accès immédiat d'un ensemble sélectionné de revues de recherche en SHS de haut niveau, l'accompagnement serait à hauteur des besoins de financement individuels de chaque revue pour accomplir ce saut, sachant qu'un nombre important d'entre elles sont déjà soutenues partiellement par les pouvoirs publics (universités, CNRS-INSHS…). Le coût de fonctionnement d'une revue est estimé, dans plusieurs études convergentes sur le coût à l'article estimé à 1000/1300 €[61], entre 20 K€ et 35 K€, en fonction du nombre d'articles publiés par an. Sur une base de 200 revues sélectionnées, le *coût maximum d'accompagnement* serait de 4 M€/an, si l'on considère un financement complet des revues, à répartir entre les établissements (dont les coûts d'abonnements aux revues concernées seraient convertis en financement « en amont » aux revues, via un dispositif à élaborer de fonds de soutien) et le Ministère, à hauteur de 1,5 M€/an à inscrire dans le cadre de sa politique de soutien aux SHS.

Par ailleurs, l'accompagnement portant sur l'aide à la traduction a été évalué, pour 50 revues sélectionnées, à environ 200 K€/an.

---

plateforme CAIRN (pour les établissements de l'ESR, le marché global est de 1,7 M€TTC/an) permettrait d'éviter une partie des pertes ainsi calculées ; des pertes éventuelles en terme de vente papier seraient compensées par l'accompagnement direct aux revues.

[61] Etudes Idate et BSN7, citées précédemment.

Article 18
Appariement de fichiers à des fins de statistique publique et de recherche scientifique et historique

1. <u>État des lieux</u>

En France, le service statistique public, défini par la loi comme l'ensemble formé par l'Insee et les services statistiques ministériels, doit fréquemment réaliser des appariements de fichiers pour produire des statistiques et des études statistiques. Les informations de nature administrative permettent de produire davantage d'information statistique de qualité tout en réduisant significativement la charge d'enquêtes auprès des ménages et des entreprises. L'objectif de mettre à contribution autant que possible les sources administratives à des fins statistiques figure pour cette raison dans le code de bonnes pratiques de la statistique européenne, inscrit dans le règlement 223/2009 relatif aux statistiques européennes.

Certains projets de recherche scientifique publics nécessitent également d'apparier des sources de données entre elles. C'est le cas par exemple lorsqu'il s'agit d'étudier les liens entre les revenus salariaux et les revenus de remplacement (chômage, indemnités journalières d'assurance maladie, retraites), les liens entre la trajectoire scolaire et la trajectoire professionnelle ultérieure d'un individu, les liens entre les épisodes de chômage et les trajectoires professionnelles pour mieux comprendre la récurrence du chômage… On peut aussi citer des projets de recherche qui s'intéressent à l'évaluation a posteriori de réformes (comme par exemple celle de la formation professionnelle) ou des projets qui s'intéressent à l'estimation complète des coûts engendrés par la prise en charge de chômeurs. Ces recherches permettraient de répondre à de nombreuses questions que se posent les pouvoirs publics ou les parlementaires au moment de prendre une décision publique ou d'adopter une nouvelle loi (notamment lors de la réalisation d'étude d'impact).

La loi de 1978 relative à l'informatique, aux fichiers et aux libertés, prévoit, dans son article 27 que l'utilisation du NIR (par exemple pour effectuer un appariement) ne peut être mise en œuvre que si le traitement a été autorisé par un décret en Conseil d'État, après avis motivé et publié de la Commission nationale de l'informatique et des libertés (Cnil), dès lors que ce traitement de données à caractère personnel est mis en œuvre pour le compte de l'État, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public.

Les administrations de l'État, en particulier celles qui composent le service statistique public, et les organismes de recherche, notamment universitaires, **doivent donc obtenir l'autorisation de ce traitement par un décret en Conseil d'État**.

Dans la pratique, l'exigence du décret en Conseil d'État s'est révélée insurmontable pour les organismes universitaires ou de recherche, puisque très rares sont ceux qui ont pu obtenir qu'un ministre prenne l'initiative de porter un décret en Conseil d'État pour permettre un appariement dans le cadre d'un projet de recherche.

Seules des administrations appartenant au service statistique public ont pu, grâce à l'appui de leur ministre de tutelle, mettre en œuvre la procédure prévue par la loi. Les démarches sont toutefois très lourdes. Cette situation conduit dans beaucoup de cas à renoncer à engager certains appariements ou à en réaliser de manière dégradée, c'est-à-dire à choisir d'apparier

les fichiers en utilisant un ensemble d'autres variables que le NIR (par exemple l'ensemble formé par le nom, l'adresse, la date de naissance etc.). Cette situation administrative entraîne donc une moindre qualité de la recherche française en sciences humaines et de l'évaluation des politiques publiques nationales.

2. Description des objectifs poursuivis

L'article vise à simplifier la procédure d'appariement dans le domaine de la statistique et de la recherche publique tout en garantissant un haut niveau de protection des données personnelles grâce à la mise en place d'un cadre de sécurité organisationnel et informatique très strict.

L'article permettrait de définir deux nouveaux dispositifs d'appariement distincts :

- **pour la statistique publique**, il s'agit de remplacer les appariements sur la base du NIR, utilisés parfois aujourd'hui, par des appariements sur la base d'une clé d'appariement non signifiante (à l'inverse du NIR, qui est signifiant puisqu'il permet de connaître directement le sexe de l'individu, ainsi que son année, son mois, son département et sa commune de naissance). La clé d'appariement, un code statistique non signifiant (CSNS), sera commune à toutes les sources statistiques. Cette clé sera changée tous les 10 ans. L'objectif est de mieux séparer les usages statistiques (utilisation du CSNS, clé d'appariement non signifiante) des usages administratifs (usage du NIR). Le choix d'un code statistique non signifiant vise à renforcer le principe d'un cloisonnement entre usage administratif et finalités de statistique publique et ainsi circonscrire l'usage des données contenant ce code au sein du seul service statistique public.
- **pour la recherche scientifique publique**, il s'agit de rendre possible les appariements de données en mettant en place les exigences de sécurité nécessaires pour leurs réalisations. Ceux-ci se feront sur la base d'une clé d'appariement non signifiante obtenue par une opération cryptographique réalisée sur le NIR. La clé associée à l'opération cryptographique sera spécifique à chaque projet de recherche : une nouvelle clé sera produite pour chaque projet de recherche. L'utilisation des données concernées contenant ce code ne sera pas possible en dehors du projet de recherche.

3. Nécessité de légiférer

3.1 Pour la statistique publique

L'article vise à permettre à la statistique publique de remplacer la procédure de décret en Conseil d'État pris après avis de la CNIL par **une procédure de déclaration à la CNIL**. Pour cela, il est nécessaire de modifier l'article 22 de la loi du 6 janvier 1978, en le complétant par un Ibis permettant de déroger au 1° du I et du II de l'article 27. La dérogation ne sera applicable que pour les traitements n'utilisant pas le NIR lui-même, mais un « code statistique non signifiant » dérivé du NIR : le présent article précise que ce code devra être créé par une opération cryptographique.

Le présent article précise également que les méthodes et le schéma organisationnel utilisés pour l'opération cryptographique devront répondre à un cahier des charges défini par un décret en Conseil d'État, pris avec avis motivé et publié de la Cnil. Le même décret en Conseil d'État précisera que l'organisme ou le service qui a effectué l'opération cryptographique, et qui donc détient la clé associée à l'opération cryptographique, ne peut avoir accès aux données confidentielles indexées par le CSNS. Ce décret sera rédigé en collaboration avec l'ANSSI.

Les données sensibles mentionnées au I de l'article 8 ou à l'article 9 de la loi du 6 janvier 1978 restent exclues du champ de l'article.

Le dispositif de création du CSNS, que le décret en Conseil d'État devra définir, reposera sur une opération cryptographique à clé secrète permettant de faire correspondre à un NIR un CSNS : ce processus permet à chaque NIR d'avoir un correspondant mais ne permet pas de recalculer le NIR d'origine à partir du CSNS en l'absence de la clé. Le CSNS aura une valeur à durée limitée dans le temps car le procédé sera répété tous les 10 ans avec des clés secrètes à chaque fois différentes. La gestion et le stockage des clés secrètes se feront dans des conditions de sécurité élevées (coffre-fort). En outre, Le CSNS resterait strictement confiné au sein du service statistique public.

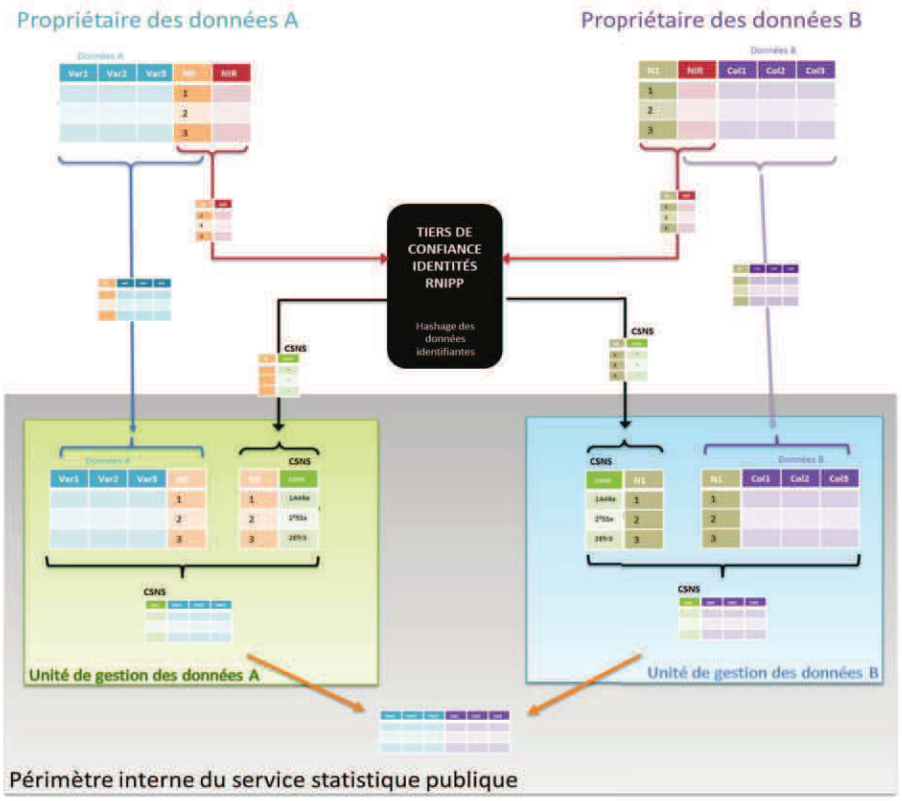
Les clés secrètes, successives dans le temps, servant à créer le code statistique non signifiant pour les travaux de la statistique publique seront détenues par les seuls gestionnaires du répertoire national d'identification des personnes physiques (RNIPP) dont la gestion est confiée à une unité dédiée au sein de l'Insee, soit une dizaine de personnes tout au plus. Elle ne serait donc pas accessible aux statisticiens de l'Insee n'appartenant pas à cette unité, ni à ceux des services statistiques ministériels.

Le schéma ci-dessous présente le processus de réalisation d'appariements sécurisés en utilisant le code statistique non signifiant (CSNS).

Les producteurs A et B transmettent d'une part les variables identifiantes (NIR ou informations permettant d'obtenir le NIR, soit les noms, prénoms, dates et lieu de naissance) ainsi qu'un code d'indexation aléatoire (N0 et N1 sur le schéma) au tiers de confiance « identités », c'est-à-dire le service de gestion du RNIPP. Ce dernier génère un code statistique non signifiant (CSNS) grâce à une opération cryptographique avec une clé secrète unique. Le CSNS est alors envoyé aux unités de gestion des données du SSP A et B. Les producteurs A et B transmettent d'autre part les variables informatives (données statistiques) et le code d'indexation aléatoire (N0 et N1 sur le schéma) aux unités de gestion des données A et B. Ceux-ci vont pouvoir créer chacun une table contenant uniquement le CSNS et les données statistiques, excluant donc les variables identifiantes. Après validation hiérarchique du besoin et déclaration à la CNIL, l'appariement des données A et B selon le CSNS pourra être réalisé.
Bien entendu, en pratique, ceci ne signifie pas que tous les statisticiens publics ont accès à tout moment à toutes les bases de données. Comme aujourd'hui, chaque équipe spécialisée sur un champ de statistiques est responsable et détentrice d'un nombre limité de fichiers. Lorsqu'un appariement entre fichiers de deux équipes distinctes apparaît nécessaire, celui-ci ne s'opère qu'après déclaration à la Cnil, donc validation hiérarchique du besoin.

Par ailleurs, le CSNS est bien sûr supprimé lorsque les données statistiques publiques sont ensuite mises à disposition des chercheurs par exemple.

Cette opération s'effectuera à chaque acquisition de nouvelles sources de données par le service statistique publique (enquête, source administrative…) mais aussi par périodicité de 10 ans pour modifier le CSNS.



3.2 Pour la recherche scientifique

L'article vise à permettre à des travaux de la recherche publique de remplacer la procédure de décret en Conseil d'État pris après avis de la CNIL par **une procédure d'autorisation auprès de la CNIL**. Lorsqu'il s'agit de données issues de la statistique publique ou de données fiscales, un projet de recherche doit d'abord être soumis au Comité du secret statistique pour obtenir la levée du secret statistique ou fiscal. Celui-ci examine notamment la finalité de la recherche proposée, la qualité des chercheurs, la sécurité mise en place, la pertinence des données dont l'accès est demandé... Cette procédure nécessite entre quatre et neuf mois. En complément du décret en Conseil d'État, un dispositif d'autorisation unique de la CNIL sera mis en place afin d'harmoniser et de sécuriser les procédures de demande et de réalisation.

L'article a pour objet de modifier l'article 25 de la loi du 6 janvier 1978, en le complétant par un 9°) permettant de déroger au 1° du I et du II de l'article 27. La dérogation ne sera applicable que pour les traitements n'utilisant pas le NIR lui-même, mais **un code recherche dédié non signifiant (CRDNS) spécifique** dérivé du NIR : le présent article précise que ce code devra être créé par une opération cryptographique.

Le présent article indique également que les méthodes et le schéma organisationnel utilisés pour l'opération cryptographique devront répondre à un cahier des charges défini par un décret en Conseil d'État, pris après avis motivé et publié de la Cnil. Ce décret définira les conditions techniques de sécurité pour la réalisation des opérations d'appariement afin de garantir la confidentialité et la traçabilité des données. Ce décret sera rédigé en collaboration avec l'ANSSI.

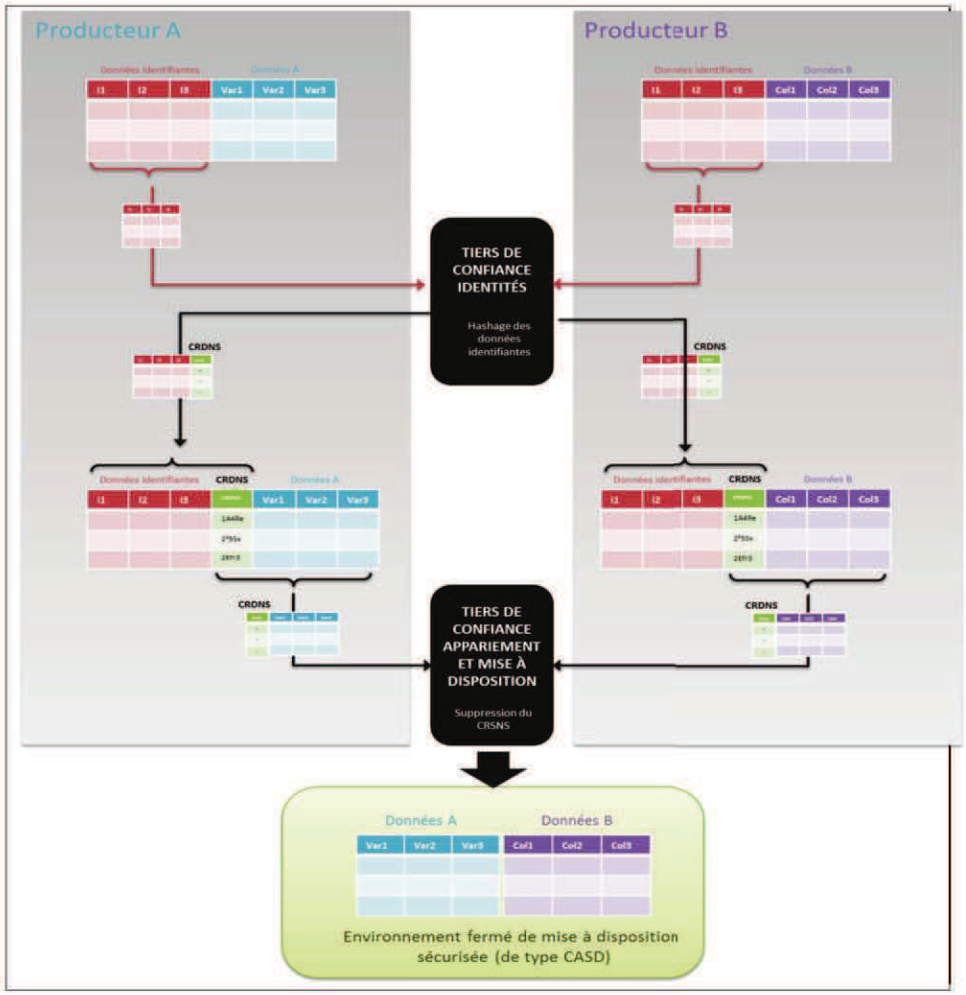
Comme pour la statistique publique, les données sensibles mentionnées au I de l'article 8 ou à l'article 9 de la loi du 6 janvier 1978 restent exclues du champ de l'article.

Contrairement à ce qui est prévu pour la statistique publique, une clé secrète différente sera créée pour chaque projet de recherche public, aboutissant à des NIR chiffrés différents pour chaque appariement. Il sera créé en conséquence pour chaque appariement, un code recherche dédié non signifiant (CRDNS) spécifique. Celui-ci serait obtenu par un procédé analogue à celui opéré pour la statistique publique, c'est-à-dire par séparation des données identifiantes des données informatives.

Le schéma ci-dessous présente de manière générique le processus de réalisation d'appariements sécurisés selon le code recherche dédié non signifiant (CRDNS).

Les producteurs A et B transmettent les variables identifiantes (NIR ou informations permettant d'obtenir le NIR, soit les noms, prénoms, dates de naissance) au tiers de confiance « identités ». Ce dernier génère un code recherche dédié non signifiant (CRDNS) grâce à une opération cryptographique avec une clé secrète spécifique au projet de recherche conservée dans des conditions de sécurités élevées par le tiers de confiance. Les variables identifiantes et le CRDNS sont alors envoyés aux producteurs. Ceux-ci créent chacun une table avec uniquement le CRDNS et les données informatives et donc suppression des variables identifiantes. Chaque producteur envoie ensuite la table résultante au tiers de confiance « appariement et mise à disposition » afin que celui-ci réalise l'appariement selon le CRDNS. Celui-ci est ensuite supprimé une fois l'opération d'appariement réalisée.

Dans ce schéma, le premier tiers de confiance n'a connaissance que des variables identifiantes et le deuxième tiers de confiance n'a connaissance que de données sans aucune information sur les identités.



4. Analyse des impacts des dispositions envisagées

4.1 Impacts pour la statistique publique

Cette mesure permettra, grâce à l'utilisation d'un code statistique non signifiant (CSNS), un meilleur usage des données entre les divers services chargés de la production au sein service statistique public, évitant en particulier des enquêtes complémentaires, coûteuses pour l'État et lourdes pour les enquêtés.

Pour la statistique publique, cette proposition aura au moins quatre impacts bénéfiques :

- *mieux séparer les usages statistiques des usages administratifs*. Le choix d'un code statistique non signifiant (CSNS) vise à renforcer le principe d'un cloisonnement entre

données à usage administratif et données traitées à des fins statistiques. Qui plus est, contrairement au NIR, le CSNS est non directement nominatif, ce qui apporte des garanties supplémentaires en termes de confidentialité lors de travaux statistiques sur les fichiers ;

- *augmenter l'efficience de la production de la statistique publique*. L'application de l'article permettra de définir un cadre mutualisé et sécurisé pour la réalisation d'appariement, ce qui augmentera l'efficacité globale de production de statistique ;
- *augmenter* la qualité de certains appariements réalisés aujourd'hui ;
- *réduire les coûts de réalisation d'étude* en limitant le recours à des enquêtes.

La faisabilité technique de ce processus ne présente pas de difficultés dans la mesure où ce type d'opération est déjà aujourd'hui réalisé au cas par cas pour chaque appariement autorisé par décret en Conseil d'État.

4.2 Impacts pour la recherche scientifique

L'impact d'une telle mesure sera considérable pour la communauté des chercheurs publics et par extension pour l'ensemble des pouvoirs publics qui bénéficieront des analyses scientifiques et objectives nouvellement possibles. En effet, cette mesure permettra de réaliser des appariements de fichiers jusqu'alors impossibles en France.

Comme pour la statistique publique, le procédé présenté est déjà mis en œuvre au cas par cas, sans harmonisation des procédures. Il est permis par autorisation de la Cnil ou décret en Conseil d'État, en particulier dans le domaine de la santé (qui restera hors du champ du présent article). La mise en place d'une organisation mutualisée et sécurisée pour la recherche scientifique optimisera les coûts de réalisation des appariements. Les coûts fixes constatés de telles opérations sont faibles et les coûts variables seront facturés aux demandeurs.

5. Consultations menées

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été consultée et ses recommandations ont été prises en compte.

Le présent article a été soumis à la CNIL et ses remarques prises en compte.

6. Textes d'application et Outre-mer

Un décret en Conseil d'État fixera les modalités d'application du présent article.

L'article 46 du projet de loi rend le présent article applicable en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans les Terres australes et antarctiques françaises.

TITRE II

La protection des droits dans la société numérique

La confiance est un facteur-clé de la croissance de l'économie numérique : confiance des usagers et des citoyens dans les services qui leur sont proposés, confiance des entreprises dans les transactions et la sécurité juridique de leurs activités. La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a défini un cadre général qui a permis un développement remarquable des services de la société de l'information. Le projet de loi entend s'inscrire dans cette continuité et, face aux nouveaux défis suscités par la seconde génération de l'internet, poser des jalons supplémentaires en faveur de la protection dans la société numérique.

Il s'agit de consolider des paramètres –clés de protection tels que :

- la neutralité et le caractère ouvert de l'internet ;
- la loyauté des plateformes ;
- la protection des données à caractère personnel et des correspondances privées.

Chapitre I[er]

Environnement ouvert

Section 1
Neutralité de l'internet

Article 19
Définition du principe de neutralité de l'internet

L'article 19 inscrit dans la loi le principe déterminant de la neutralité de l'internet : il définit et énonce une règle structurante qui doit gouverner le fonctionnement du réseau numérique. La neutralité de l'internet est une composante essentielle à la confiance et à la protection des usages et de l'innovation dans l'écosystème numérique.

1. **État des lieux**

1.1 Principe de neutralité

Lors de la révision en 2009 du cadre réglementaire européen des communications électroniques *« Paquet télécom »,* des mesures concrètes ont été adoptées concernant la neutralité des réseaux. Transposées en droit français dans le code des postes et des communications électroniques et dans le code de la consommation par l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, ces mesures s'articulent autour de trois axes :

- le renforcement de la transparence et de l'information des consommateurs concernant les pratiques de gestion de trafic mises en œuvre par les opérateurs de communications électroniques (art. L. 121-83 et L. 121-83-1 du code de la consommation) ;

- la possibilité pour les pouvoirs publics d'intervenir dans les relations entre les opérateurs de communications électroniques et les fournisseurs de services de communication au public en ligne concernant les conditions d'acheminement du trafic (art. L. 32-4 et L. 36-8 du code des postes et des communications électroniques) ;
- la garantie du service et la préservation de l'internet dit « *best effort* » (art. L. 32-1 et L. 36-6 du même code).

Le règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'internet ouvert et modifiant la directive 2002/22/CE sur le service universel et les droits de l'utilisateur concernant les réseaux de communication et les services et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union, dit règlement « Marché unique des télécommunications » ou MUT, précise notamment les règles en matière de neutralité de l'internet.

1.2 Pouvoirs de l'ARCEP

Le pouvoir d'enquête est un des fondements essentiels de la régulation du secteur des communications électroniques par l'Autorité de régulation des communications électroniques et des postes (ARCEP).

Le recueil d'informations auprès du secteur permet entre autres à l'Autorité de mettre en œuvre son pouvoir de sanction lorsque cela est nécessaire au respect du cadre réglementaire.

En 2011, le pouvoir d'enquête prévu à l'article L. 32-4 du code des postes et des communications électroniques a été complété dans le cadre de la transposition en droit français des directives 2009/136/CE et 2009/140/CE du 25 novembre 2009 dites « *Paquet télécom de 2009* » afin de lui permettre de recueillir des informations auprès des opérateurs mais également auprès des fournisseurs de services de communication au public en ligne, notamment en cas de demande de règlement d'un différend portant sur les conditions techniques et tarifaires d'acheminement du trafic.

S'agissant du pouvoir de sanction, l'ordonnance n° 2014-329 du 12 mars 2014 relative à l'économie numérique a permis le rétablissement du pouvoir de sanction de l'ARCEP en tirant les conséquences de la décision du 5 juillet 2013, par laquelle le Conseil constitutionnel avait estimé que les dispositions législatives relatives au pouvoir de sanction de l'ARCEP dans le secteur des communications électroniques n'étaient pas conformes à la Constitution.

En l'état du droit, l'action de sanctionner intervient à la suite d'un manquement. Or l'ARCEP ne doit pas s'envisager comme un seul juge des manquements, mais un régulateur chargé d'accompagner le développement du secteur. C'est pourquoi l'ARCEP doit pouvoir agir en amont et en particulier vérifier le respect des obligations de déploiement et d'investissement pour s'assurer de la compatibilité des trajectoires de déploiement de réseaux mobiles avec les obligations de couverture prévues dans les autorisation d'utilisation de fréquences des opérateurs.

Par ailleurs, l'article L. 36-11 du code des postes et des communications électroniques permet de sanctionner les opérateurs qui ne respecteraient pas une décision prise par l'ARCEP dans le cadre d'un règlement de différends. Dans la mesure où l'ARCEP peut régler non seulement les différends entre deux opérateurs de communications électroniques mais également entre

un opérateur de communications électroniques et un fournisseur de services de communication au public en ligne (FSCPL) à la demande de l'un ou l'autre des acteurs.

2. Description des objectifs poursuivis

Afin de consolider l'approche harmonisée de la neutralité de l'internet retenue au niveau européen dans le cadre du règlement « *marché unique des télécommunications* », le projet de loi inscrit le respect de la neutralité de l'internet, d'une part, dans les objectifs auxquels doivent veiller le ministre chargé des communications électroniques et l'ARCEP (I de l'article 19) et, d'autre part, au nombre des obligations s'imposant aux exploitants de réseaux ouverts au public et aux fournisseurs de services de communications électroniques (III de l'article 19).

Afin de garantir le caractère ouvert d'internet, il est proposé de préciser que les demandes d'informations peuvent porter non seulement sur l'acheminement mais aussi sur la gestion du trafic (II de l'article 19). Cette modification de l'article L. 32-4 du code des postes et des communications électroniques permettra à l'ARCEP de disposer des fondements juridiques lui permettant de demander des informations aux opérateurs sur les pratiques de gestion de trafic qu'ils mettent en œuvre et de s'assurer ainsi qu'ils respectent les dispositions du règlement européen « marché unique des télécommunications ».

Il s'agit ensuite d'assurer l'égalité de traitement dans les droits et obligations des opérateurs et des FSCPL face aux décisions prises par le régulateur dans le cadre d'un règlement de différend.

Il s'agit enfin, relativement aux obligations de déploiement de réseaux d'opérateurs, de permettre une action préventive de l'ARCEP. Cette dernière avait noté dans son rapport annuel pour l'année 2011, que l'attente d'un constat d'échec ou d'une inexécution, à la date à laquelle l'obligation doit être réalisée, pour mettre en demeure l'opérateur, entraine mécaniquement un report du calendrier initial, à l'instar des situations connues dans le passé pour les mises en demeure relatives aux obligations de couverture des réseaux mobiles de troisième génération. Les retards dans les déploiements des réseaux ne doivent pas être constatés mais anticipés. Aussi pour inciter et accompagner les opérateurs à suivre une trajectoire leur permettant d'atteindre les obligations à la date fixée, il convient de permettre à l'Autorité d'user de son pouvoir de sanction pour mettre en demeure l'opérateur concerné, avant l'échéance en cause, de se conformer à ladite échéance. Dans le contexte du déploiement des réseaux mobiles de troisième et quatrième générations, il est particulièrement important que l'ARCEP puisse s'assurer en temps utile du respect par les opérateurs de leurs obligations (4° du VI de l'article 19).

3. Options possibles et nécessité de légiférer

Avec le développement de services innovants nécessitant une qualité supérieure, il est primordial d'encadrer strictement le principe de neutralité de l'internet, les mesures de gestion de trafic et l'impact que ces services spécialisés peuvent avoir sur la fourniture des services d'accès à Internet. Il ne faut pas qu'un fournisseur de service d'accès à internet puisse mettre en œuvre des mesures non justifiées qui limitent l'accès des consommateurs à l'internet ouvert.

Les modalités d'application du principe de neutralité peuvent s'envisager par un accroissement des pouvoirs de l'ARCEP. Les pouvoirs d'enquête peuvent porter atteinte à des libertés fondamentales garanties par la Constitution. A cet égard, ils doivent être strictement encadrés par la loi, c'est pourquoi la modification de l'étendue des pouvoirs d'enquête ne peut relever que du seul niveau législatif.

Le pouvoir de sanction de l'ARCEP ayant fait l'objet de contestation par le passé, il est désormais décrit dans des dispositions législatives qui garantissent la sécurité juridique de ses décisions. Ce pouvoir est d'ailleurs encadré par des principes issus de la Convention européenne des droits de l'homme. Le niveau de norme attaché au respect de ces principes relève du domaine législatif.

4. Analyse des impacts des dispositions envisagées

1. L'ARCEP a déjà largement mis en œuvre ses pouvoirs d'enquête et le recensement des pratiques de gestion de trafic a permis de dissuader les comportements inappropriés si bien que les blocages très répandus auparavant (ex : blocage de la « *VoIP* » et du « *P2P* » sur le mobile) ont totalement disparu. L'Autorité n'a donc pas eu, jusqu'ici, besoin de sanctionner un opérateur en raison des mesures de gestion de trafic mise en œuvre. Cependant l'inclusion dans le code des postes et des communications électroniques d'une définition claire de la neutralité de l'internet est de nature à promouvoir l'innovation sans remettre en cause les fondements de l'internet ouvert.

2. L'extension du pouvoir d'enquête n'engage pas de charge supplémentaire immédiate pour les autorités concernées ou les entreprises en cause. Ces derniers disposeront simplement de la faculté de recueillir davantage d'informations lorsque cela est nécessaire. Les dispositions correspondantes visent surtout à consolider juridiquement ce pouvoir d'enquête.

Le renforcement du pouvoir de sanction de l'ARCEP n'engage pas de charge supplémentaire immédiate pour cette dernière. Il s'agit d'une mesure de bonne administration qui vise à garantir la sécurité juridique des décisions de l'Autorité ainsi que l'égalité de traitement des acteurs du secteur des communications électroniques. Aucune dépense spécifique n'est nécessaire pour ce faire.

5. Consultations menées

Cet article a été soumis pour avis à l'ARCEP, en application de l'article L. 36-5 du code des postes et des communications électroniques, et à la Commission supérieure du service publique des postes et des communications électroniques, en application de l'article L. 125 du même code.

Article 20
Auto-hébergement

Le projet de loi introduit dans le code des postes et des communications électroniques une nouvelle disposition qui doit permettre à tout utilisateur d'héberger, par les moyens qu'il entend, ses propres données, en utilisant le réseau fournit par l'opérateur de communications électroniques. L'article est rédigé sous la forme d'une interdiction pour les opérateurs, de mettre en place des mesures techniques visant à empêcher l'utilisateur d'accéder à des données stockées sur un équipement approprié et connecté directement ou indirectement à Internet, via le service d'accès auquel il s'est abonné et via la « box » dont il dispose.

1. État des lieux

De plus en plus d'utilisateurs entendent héberger eux-mêmes leurs données par l'acquisition d'un serveur de donnée personnel. De cette sorte, ils sont maître du stockage et de la conservation de leurs données et peuvent y définir des règles d'accès, notamment à distance. Cette pratique assure un contrôle supplémentaire pour les utilisateurs de leurs données. Pour ce faire, ils doivent connecter ce serveur personnel à la « box » internet fournie par le fournisseur d'accès à internet.

Or certains fournisseurs d'accès à Internet français ne permettent pas d'héberger derrière la « box », un serveur personnel de données. Cette pratique s'observe, par exemple, lorsque des ports internet sont bloqués ou lorsque des adresses IP dynamiques sont allouées. L'installation d'un serveur chez soi requiert d'effectuer des opérations techniques de redirection de trafic de la « box » vers le serveur. L'allocation d'une adresse IP dynamique ou une limitation dans l'usage des ports internet empêchent cette redirection et donc la mise en place d'un serveur personnel. Or un utilisateur final doit avoir la liberté d'héberger par ses propres moyens, les informations qu'il traite, en particulier celles à caractère personnel (les courriels, les calendriers, les contacts, la messagerie instantanée...). Pour garantir cette liberté aux utilisateurs, il convient de s'assurer que les opérateurs ne mettent pas en œuvre des techniques empêchant l'hébergement par l'utilisateur de ses propres données. Aussi, la disposition interdit aux opérateurs de services de communications électroniques de limiter les services que peut mettre en place l'utilisateur pour ses propres besoins.

2. Objectifs poursuivis

La nouvelle disposition doit permettre à l'utilisateur de disposer librement de ses données en lui permettant d'héberger lui-même ses données. L'objectif est de conforter le pouvoir de l'individu de décider lui-même des méthodes de gestion de ses données. L'article s'inscrit ainsi dans le prolongement de l'article 26 qui inscrit le principe de libre disposition de ses données personnelles dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3. Options possibles et nécessité de légiférer

Comme pour la neutralité du net, avec le développement de services innovants et du marché des données, il est primordial de garantir strictement la liberté des utilisateurs en interdisant

aux opérateurs de mettre en œuvre les mesures techniques de nature à limiter les capacités de contrôle des utilisateurs. La garantie de cette liberté relève du niveau législatif.

4. Analyse des impacts des dispositions envisagées

Certains opérateurs de communications électroniques, particulièrement attachés à la liberté des utilisateurs n'opposent déjà aucune résistance ni aucun blocage technique pour l'auto-hébergement. Il peut s'agir également d'une voie pour l'innovation en offrant des services supplémentaires à un utilisateur. En revanche, d'autres opérateurs, notamment pour des raisons de gestion de trafic limitent les capacités techniques des équipements chez l'utilisateur (la box).

Pour ces derniers, des développements logiciels seront nécessaires pour rajouter des fonctionnalités ou options. Une mise à jour logicielle sera donc nécessaire. Elles pourront se faire de manière très progressive, car tous les utilisateurs ne possèdent pas leur propre serveur. Aussi cette mise à jour présente un coût très marginal.

5. Consultations menées

Cet article a été soumis pour avis à l'ARCEP, en application de l'article L. 36-5 du code des postes et des communications électroniques, et à la Commission supérieure du service publique des postes et des communications électroniques, en application de l'article L. 125 du même code.

Section 2
Portabilité et récupération des données

L'impératif de protection dans le numérique, c'est aussi l'assurance nécessaire pour les usagers et les entreprises d'être toujours en capacité de changer de fournisseur. Les situations « d'enfermement » où les utilisateurs des services numériques sont prisonniers de leurs fournisseurs sont préjudiciables tout autant à la liberté de choix individuelle qu'à l'efficience du marché. Il s'agit ainsi de garantir le caractère concurrentiel du marché et de réduire les barrières à la mobilité des utilisateurs.

Article 21
Portabilité et récupération des données

Le projet de loi introduit une nouvelle règle destinée à faciliter la fluidité des offres et services numériques en permettant à tout utilisateur de récupérer à tout moment, en toutes circonstances et sans justification les données qui ont été communiquées dans le cadre des services fournis, afin éventuellement de les transférer à tout autre fournisseur alternatif.

L'article vise en tout premier lieu les services de courrier électronique pour le grand public, qui constituent un service de référence essentiel dans les usages numériques. Le dispositif de portabilité est également conçu en faveur des consommateurs et des entreprises déposant des données en ligne.

1. <u>État des lieux</u>

1.1. Eléments économiques

1.1.1 Concernant les courriels

L'envoi et la réception de courrier électronique est l'une des utilisations les plus courantes d'internet : selon une étude Médiamétrie de 2014 43,2 millions de Français utilisent régulièrement Internet, et 95% d'entre eux consultent quotidiennement une messagerie électronique, sur ordinateur personnel mais aussi de plus en plus à partir de leur mobile et de leur tablette.

Deux types d'entreprises proposent des services de courrier électronique, permettant de recevoir, envoyer et stocker des courriels : les fournisseurs d'accès internet (FAI), le service étant lié à l'abonnement, et les « *pure players* » d'internet (ou OTT : over the top), qui proposent ce service sans lien avec un service d'accès à l'internet. La plupart des services de courrier électronique sont aujourd'hui gratuits pour les consommateurs, ou inclus dans l'offre de base d'accès à l'internet, et ne sont payants que si l'on souhaite dépasser une limite de stockage (100 Go pour Yahoo par exemple) qui concerne presque essentiellement les professionnels. Les opérateurs « *pure players* » qui proposent ces services le plus souvent gratuitement et se rémunèrent notamment grâce à la publicité.

L'article concerne uniquement les fournisseurs d'un service de courrier électronique comprenant la mise à disposition d'une adresse électronique. Les services de messagerie électronique tels que Skype, ainsi les messageries privées, par exemple celles mises en place

par les banques pour communiquer avec leurs clients dans l'espace en ligne ne sont pas soumises aux dispositions de cet article.

1.1.2 Concernant les données stockées en ligne

Le *cloud computing* (informatique dans les nuages), apparu au cours des années 2000, consiste à délocaliser des données, des fichiers et des utilisations des ordinateurs des particuliers et des entreprises vers le « nuage (cloud) internet », c'est-à-dire vers des serveurs extérieurs, qui hébergent les données, les fichiers et les applications utilisées par le client.

Le cloud intéresse de plus en plus les particuliers et les entreprises. Il permet notamment de disposer de capacités de stockage supplémentaires, réduit les investissements en matériel informatique des entreprises, et permet plus de souplesse dans la gestion des données, ce qui intéresse particulièrement les PME. Il offre de plus la possibilité de confier un certain nombre de tâches (comptabilité par exemple, ou gestion de la clientèle) à des services en ligne, permettant ainsi aux entreprises d'alléger leur gestion informatique.

Le *cloud computing* est de ce fait en plein essor. En 2014 le marché français du cloud était estimé à près de 5 milliards[62] d'euros, contre 2,3 milliards en 2009. Le cloud est d'après toutes les études prospectives appelé à se développer de manière exponentielle dans les années à venir. Il s'agit d'un des rares domaines du numérique où les entreprises européennes (SAP, Orange) conservent pour l'instant une part de marché appréciable par rapport aux géants américains (Google, Amazon et Microsoft en tête). La pénétration du *cloud computing* en France est pourtant plus lente que dans les autres pays européens : en 2014, 12% des entreprises d'au moins 10 personnes implantées dans l'Hexagone ont acheté des services d'informatique en nuage, contre 19% en moyenne en Europe. La France se classe ainsi loin, à la 21e place, des utilisateurs de cloud dans l'Union européenne[63].

1.2. Eléments juridiques

1.2.1. Concernant les courriels

Il n'existe pas de disposition spécifique concernant la portabilité des courriels. Seul l'article L. 44-1 du code des postes et des communications électroniques approche le sujet, en prévoyant que les fournisseurs d'accès à internet doivent permettre à leurs clients qui changent d'opérateur de conserver gratuitement un accès aux messages reçus sur leur boite aux lettres électronique attribuée sous leur nom de domaine durant six mois.

Par ailleurs, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a introduit différentes dispositions dans le code civil (articles 1369-1 et suivants), qui confèrent une valeur juridique aux courriers électroniques dans le cadre d'un contrat.

---

[62] Source : http://www.zdnet.fr/actualites/chiffres-cles-le-marche-du-cloud-computing-39790256.htm

[63] Source : http://www.new.plusquelinfo.com/DisplayService/DisplayService.aspx?pmcrypt=oL3Fq2%2fyJf7Mruvrflj8onu0T0vm8bO8bJkUQRJk6ViQ%2bNmwLYOi%2fiZOEnomZHNafs7CX%2bfwsIry2s7FP66hjWvGgo4G%2f9Ni6SGwkz1Xe2Lb8bFVa8ORnIAuvA0fwUQZ&Referer=0&s=20017718-p-33472181

1.2.2. Concernant les données stockées en ligne

Les activités de *cloud computing* sont soumises en partie à la législation en vigueur concernant les activités numériques, et notamment la loi n° 78-17 du 6 janvier 1978 Informatique et Libertés, en matière de protection des données personnelles, et la loi n° 2004-575 du 21 juin 2004 sur la confiance en l'économie numérique (en particulier son article 19 dressant la liste des informations obligatoirement fournies par le professionnel au consommateur dans le cadre d'un contrat conclu par voie électronique). Les contrats de *cloud* sont soumis aux dispositions du code civil régissant l'ensemble des contrats, ainsi qu'aux articles L. 121-16 et suivants du code de la consommation concernant les dispositions relatives aux ventes de biens et fournitures de prestations de services à distance.

Aucune mesure spécifique au *cloud computing*, notamment concernant la récupération des données, n'existe cependant à ce jour.

2. Description des objectifs poursuivis

Le projet de loi a pour objectif principal de réduire la viscosité du marché en instaurant pour les clients de services numériques majeurs tels que le courriel, le *cloud computing* et les services en ligne associé à un compte utilisateur, un droit de récupérer et transférer leurs données aisément.

La perspective de perdre ses données ou de devoir se lancer dans une fastidieuse récupération manuelle de celles-ci peut en effet inciter le consommateur à renoncer à changer d'opérateur, quand bien même il ne serait plus satisfait de ses services. Le projet de texte permettra de lever cette barrière et améliorer ainsi le fonctionnement du marché, favoriser la concurrence et l'essor de nouveaux services innovants tout en offrant au consommateur une mobilité numérique accrue.

L'article L. 121-120 pose donc le principe d'un droit à la portabilité, à tout moment et sans justification.

2.1 Dispositions concernant les courriels

Le nouvel article L. 121-121 du code de la consommation, créé par le projet de loi, vise à favoriser la portabilité des services de courrier électronique. Il impose à l'opérateur de service de courrier électronique d'offrir au consommateur la possibilité de transférer sur un autre service ses courriels, ainsi que sa liste de contacts. Le dernier alinéa étend en outre l'obligation d'accès gratuit au courrier électronique reçu sur l'adresse électronique attribuée sous son nom de domaine durant six mois qui ne concernait jusqu'à présent que les FAI à tous les opérateurs de services de courrier électronique.

Plusieurs dispositions ont été prévues afin de garantir l'effectivité de cette portabilité :

- gratuité de la fonctionnalité ;
- référence à une migration « directe » (pour simplifier l'opération en ne se limitant pas à des fonctions d'exportation vers ou d'importation depuis le disque dur) ;

- définition d'une obligation dans la limite des capacités de stockage de la boîte de courrier électronique de destination (l'opérateur pouvant toujours proposer un service premium payant avec une capacité plus importante) ;
- édiction d'une obligation de transmission des informations techniques nécessaires entre opérateurs (plutôt que l'instauration d'un mécanisme plus lourd de coopération horizontale pouvant soulever des difficultés sous l'angle de la concurrence et de mise en œuvre pour certains opérateurs étrangers).

2.2 Dispositions concernant les données stockées en ligne

Le nouvel article L. 121-122 du code de la consommation, créé par le projet de loi, vise à favoriser la portabilité des données en *cloud* et celles associées aux comptes utilisateurs des services de communication en ligne.

Le développement de l'économie de l'infonuagique peut rendre les utilisateurs dépendants d'un fournisseur de service. Qu'il s'agisse du stockage de ses fichiers personnels en ligne, notamment de fichiers vidéos sur des plateformes, ou de traitement de données en ligne, l'utilisateur qui a importé une quantité importante de données personnelles peut hésiter à changer de fournisseur si ces données, qu'il n'a par ailleurs pas forcément conservées sur un serveur personnel, sont difficilement récupérables, ou récupérables dans un format incompatible avec un traitement par un autre fournisseur de service.

Par ailleurs la multiplication des services de communication en ligne s'est accompagnée d'une personnalisation croissante de ceux-ci. Beaucoup de services numériques sont désormais associés à un compte utilisateur qui enregistre les données liées à l'utilisation du service. Dans ce cas il est important pour le consommateur pour pouvoir passer d'un service à un autre d'être en mesure de récupérer les données liées à son compte utilisateur et résultant de son usage du service : playlists, albums de photos personnelles, historique de navigation ou d'achat, données de géolocalisation par exemple.

La disposition fait obligation aux fournisseurs d'un service de communication au public en ligne de proposer une fonctionnalité permettant la récupération aisée des fichiers déposés par le consommateur et les données associées à son compte utilisateur. Cette récupération des données doit être possible par requête unique ou au moins par type ou format de fichiers, afin d'éviter une procédure de récupération difficile ou fastidieuse à mettre en œuvre (par exemple effectuée fichier par fichier).

Quand les données sont saisies et traitées en ligne, il n'est pas toujours possible de récupérer les données brutes, qui peuvent être intégrées dans des fichiers d'un format propriétaire (cas par exemple d'un logiciel de comptabilité en ligne ou d'un service en ligne élaborant des plans et visualisations en trois dimensions à partir de cotes saisies par le consommateur). Dans ce cas, le dernier alinéa de l'article L. 121-122 fait obligation au service en ligne d'informer clairement l'utilisateur sur les difficultés éventuelles pour récupérer les données et, si une forme de récupération est possible, sur la procédure et la forme sous laquelle les données sont récupérables.

2.3 Dispositions communes

La sous-section 3 a pour objectif :

- d'étendre aux professionnels l'ensemble des dispositions précédentes. En effet ces obligations de portabilité visent des services à destination des consommateurs, mais également proposés à des professionnels. S'agissant du *cloud computing*, les barrières de marché dues à la difficulté de récupération ou portabilité des données concernent d'ailleurs notablement les entreprises ;
- de mettre en place des sanctions pour garantir l'effectivité du dispositif ;
- de renvoyer à un décret la fixation d'un seuil d'application des dispositions du présent article. En effet l'obligation de portabilité pourrait créer des contraintes trop lourdes pour des PME à leur création ou des entreprises dont l'activité en ligne n'est que secondaire. Le nouvel article L.121-125 du Code de la consommation confie donc à un décret le soin de définir le seuil en deçà duquel la portabilité n'est pas obligatoire. Ce seuil sera exprimé en nombre de comptes utilisateur actifs, qui est le meilleur moyen de mesurer l'activité d'un site en ligne.

3. Options possibles et nécessité de légiférer

3.1 Concernant les courriels

Du fait du caractère juridiquement opposable des courriels depuis loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, il est nécessaire pour les consommateurs et les entreprises de pouvoir bénéficier gratuitement de la portabilité des courriers électroniques. Or les opérateurs concernés sont a priori peu disposés à offrir cette fonctionnalité sur simple requête de consommateurs, ce qui demande par ailleurs des échanges d'informations techniques entre eux. De ce fait, seule une intervention des pouvoirs publics semble à même de réaliser cet objectif afin d'en poser le principe et d'en définir les modalités (conditions techniques pour assurer l'interopérabilité, par exemple).

3.2 Concernant les données stockées en ligne

Le choix d'externaliser une solution informatique dans le cloud implique une perte de maîtrise sur cette solution durant la période contractuelle et pose nécessairement la question des modalités de récupération de cette maîtrise à l'issue du contrat. Or le cloud est très utilisé par les PME, qui représentaient en 2014 selon l'INSEE plus des trois quarts des acheteurs de services de cloud.

Les PME n'ont souvent pas les moyens humains et matériels de négocier les contrats avec les opérateurs de service du cloud à leur avantage, et ont du mal à récupérer leurs données lorsqu'elles souhaitent migrer vers un autre service. Ces considérations freinent d'ailleurs la diffusion de l'utilisation du cloud en France par les entreprises. Une intervention des pouvoirs publics se justifie donc parfaitement au regard des potentialités de croissance du cloud et des viscosités actuelles du marché.

Dans le cadre de l'agenda numérique, la Commission européenne s'intéresse à une possible réglementation des contrats du cloud. Un groupe d'experts a été lancé en juin 2013. Compte tenu de l'importance du sujet, et de la vitesse de son évolution, il apparait toutefois préférable

d'adopter une réglementation nationale rapidement, dans l'attente d'une éventuelle initiative européenne qui ne saurait prospérer avant plusieurs années.

3.3 Options retenues

Selon l'article 34 de la Constitution : *« La loi détermine les principes fondamentaux : […] du régime de la propriété, des droits réels et des obligations civiles et commerciales ».*

La mise en place d'obligations pesant sur les fournisseurs de services numériques est donc du domaine de la loi.

Le projet de loi vise à favoriser la portabilité des services de courrier électronique et des données et fichiers liées au *cloud computing*. Il s'agit d'une mesure de protection des consommateurs : il semble préférable de l'insérer à titre principal dans le Code de la consommation, au chapitre Ier du titre II du Livre premier, chapitre qui traite des pratiques commerciales réglementées.

4. Analyse des impacts des dispositions envisagées

4.1 Concernant les courriers électroniques

4.1.1 Portabilité des courriels et contacts

- Pour les services de courrier électronique

Il est difficile d'évaluer les surcoûts engendrés par cette mesure pour les services de courrier électronique. La migration des courriels et des carnets d'adresse ne devrait toutefois pas nécessiter des dépenses majeures, à l'heure du déploiement du très haut débit. L'on estime que les coûts de développement informatique nécessités par la mesure demeurent dans des budgets accessibles, de l'ordre de quelques dizaines de milliers d'euros, pour des opérateurs très majoritairement de grande envergure (qu'il s'agisse de fournisseurs d'accès à Internet ou de *pure players* d'Internet).

La fluidification du marché induite par cette disposition doit par ailleurs permettre une plus grande concurrence et donc des gains d'efficience du marché, un meilleur développement économique des acteurs et l'essor de nouveaux services innovants.

- Pour les consommateurs

La mesure proposée réduit le risque juridique qu'engendre une migration d'un service de courrier électronique vers un autre du fait de la valeur légale reconnue aux courriers électroniques. L'impact économique est difficile à évaluer mais sans doute faible pour les consommateurs, du fait de la prédominance des services de courrier électronique gratuits.

Les entreprises dont l'utilisation des services de courrier électronique est intensive, et qui ont recours à des solutions payantes, devraient pouvoir bénéficier d'un léger gain, cette mesure diminuant la viscosité du marché et leur conférant un pouvoir de négociation accru face aux opérateurs.

4.1.2 Maintien de l'accès aux services de courrier électronique après résiliation

Le maintien d'un accès gratuit au courrier électronique reçu six mois après résiliation ne devrait avoir qu'un impact limité, les consommateurs disposant d'un service de courrier électronique lié à leur accès internet étant déjà couverts par l'article L. 44-1 du code des postes et des communications électroniques, qui se trouve élargi à l'ensemble des services de courriel par la présente mesure.

En diminuant là aussi la viscosité du marché pour les entreprises, qui verront moins d'obstacles à un changement de service courriel, la mesure pourra améliorer la position des entreprises françaises, notamment les PME, dans leurs négociations d'achat de services informatiques.

4.2 Concernant les données stockées en ligne

4.2.1 La récupération des fichiers et des données utilisateurs en une requête unique

- Pour les opérateurs

Les opérateurs devront développer une fonctionnalité permettant au consommateur en une requête unique, ou au moins par fichier ou type de format, de récupérer les fichiers et les données qu'il a déposés ou qui résultent de son utilisation du service. Le coût d'un tel développement dépend des systèmes d'information considérés, mais il devrait être limité, compte tenu du fait que toutes les informations relatives à un compte utilisateur données étant par définition en possession des opérateurs.

En outre, la création d'un seuil d'application permettra de ne pas pénaliser les entreprises à leur création ou celles dont l'activité en ligne est marginale.

La disposition permet d'exclure les cas dans lesquels la portabilité ou la récupération des fichiers sont susceptibles de soulever des difficultés techniques disproportionnées (par exemple pour des questions de format de fichier) ainsi que les possibles atteintes à la propriété intellectuelle.

- Pour les consommateurs et les entreprises clientes

En rendant plus facile la rupture d'un contrat de cloud, la mesure proposée permettra de diminuer la viscosité du marché, et favoriser notamment le recours au cloud par les entreprises. Même si, selon une étude d'un cabinet privé[64], la sécurité arrive largement en tête des motivations des entreprises n'ayant pas recours au cloud, la portabilité fait partie des préoccupations majeures suscitées par un recours au cloud. La mesure proposée favorisera donc la croissance du *cloud computing* en France.

[64] Disponible sur le site cloudindex.fr : http://www.cloudindex.fr/sites/default/files/PAC%20CloudIndex%20-%20Analyse%20de%CC%81cembre%202014.pdf

4.2.2 L'information sur la restitution des données traitées en ligne

Aucun coût ni impact macro-économique significatif ne semblent pouvoir être associés à cette mesure, mais elle contribuera elle aussi à réduire à la marge la viscosité du marché, en améliorant l'information du consommateur et des entreprises clientes.

5. Consultations menées

Le Conseil national du numérique, à la demande du Premier ministre, a lancé une concertation nationale sur le numérique, afin d'associer les citoyens à la préparation du projet de loi. Cette concertation, menée en ligne et à travers plusieurs rencontres, pendant cinq mois (octobre 2014- février 2015) a conduit à l'élaboration d'un rapport remis au Premier ministre le 18 juin 2015.

Le sujet plus général de la portabilité des données est évoqué plusieurs fois dans les conclusions de la consultation. Parmi les 70 recommandations du rapport, on notera notamment la 4e qui s'intitule : « Favoriser la maîtrise et l'usage de leurs données par les individus ». L'un de ses paragraphes est consacré à « un droit effectif à la portabilité des données ».

6. Textes d'application et Outre-mer

Un décret fixera le seuil du nombre d'utilisateurs ayant fait l'objet d'une connexion au cours des douze derniers mois pour les fournisseurs de service de communication au public en ligne.

L'article 46 du projet de loi rend le 1° du I et le II de l'article 21 applicable à Wallis et Futuna. L'article 47 modifie en conséquence l'article L. 123-1 du code de la consommation.

Section 3
Loyauté des plateformes

Consolider les règles de protection dans la société numérique nécessite aussi de répondre aux nouveaux défis posés par le développement d'acteurs numériques puissants, qui, compte-tenu de leur pouvoir de marché et de leur audience incontournable, sont susceptibles de biaiser à leur avantage le fonctionnement du marché. Ces nouvelles « plateformes numériques » actives sur un grand nombre de segments (réseaux sociaux, commerce en ligne, moteurs de recherche, magasins d'applications, tourisme en ligne…) opèrent sur le marché dans le cadre du droit commun de la régulation économique (essentiellement le code de commerce). Au regard des enjeux critiques en cause, il apparaît aujourd'hui nécessaire de renforcer les obligations de loyauté applicables à ces nouveaux acteurs.

Article 22
Principe de loyauté vis-à-vis des consommateurs

Le projet de loi énonce une nouvelle obligation générale de loyauté de l'information vis-à-vis des consommateurs. Le projet de loi adopte également une définition générique de ces opérateurs de plateforme en ligne qui permet d'appréhender la globalité des évolutions en cours.

1. <u>État des lieux</u>

Comme l'a précisé le Conseil d'État dans son étude annuelle de 2014 *« le numérique et les droits fondamentaux », « deux catégories d'acteurs jouent un rôle particulièrement important dans la diffusion des contenus sur internet : les opérateurs de communications électroniques qui les acheminent vers les utilisateurs finaux ; les plateformes qui proposent des services de référencement et de classement indispensables pour faire le tri dans la masse des informations et services disponibles ».*

Or, en l'état actuel de la réglementation, les consommateurs ne disposent pas d'informations suffisamment précises et transparentes sur les règles de référencement et de classement mises en œuvre par certains professionnels.

L'article 134 de la loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques a toutefois inséré dans le code de la consommation à l'article L. 111-5-1 une nouvelle disposition qui prévoit que « *sans préjudice des obligations d'information prévues à l'article 19 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, toute personne dont l'activité consiste à mettre en relation, par voie électronique, plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un bien ou d'un service est tenue de délivrer une information loyale, claire et transparente sur les conditions générales d'utilisation du service d'intermédiation et sur les modalités de référencement, de classement et de déréférencement des offres mises en ligne.*

Lorsque seuls des consommateurs ou des non-professionnels sont mis en relation, la personne mentionnée au premier alinéa du présent article est également tenue de fournir une information loyale, claire et transparente sur la qualité de l'annonceur et les droits et obligations des parties en matière civile et fiscale. « Lorsque des professionnels, vendeurs ou prestataires de services sont mis en relation avec des consommateurs, la personne mentionnée au premier alinéa du présent article est également tenue de mettre à leur disposition un espace leur permettant de communiquer aux consommateurs les informations prévues à l'article L. 121-17 ».

Ainsi, le législateur a-t-il souhaité rendre plus transparente et loyale l'information à destination des consommateurs à l'occasion d'une mise en relation en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un bien ou d'un service. Ce principe inscrit dans la loi est limité aux mises en relation opérées soit dans le cadre des places de marchés (« *marketplace* ») soit à l'occasion d'une consommation dite collaborative entre consommateurs. A ce titre, un groupe de travail spécifique aux plateformes et à l'économie collaborative a été mis en place au sein du conseil national de la consommation composé paritairement de représentants d'associations de consommateurs et de représentants de professionnels. Les travaux devront permettre au Gouvernement de prendre le décret d'application mentionné dans la loi du 5 aout précitée.

Toutefois, en dehors de cette disposition, les plateformes ne sont pas précisément définies en droit et relèvent globalement des services de la société de l'information tels que définis par la directive 2000/31 ainsi que par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique sans qu'un principe général de loyauté et de transparence soit inscrit dans le code de la consommation. C'est pourquoi, le présent article propose de définir la notion d'opérateur de plateforme en ligne lorsqu'elle intervient dans le cadre exclusivement de la consommation et d'inscrire un principe de loyauté et de transparence et de préciser certaines informations fondamentales sur lesquelles il convient que l'information des consommateurs soit particulièrement claire.

2. Description des objectifs poursuivis

Dans ce cadre et dans le respect de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects techniques des services de la société de l'information et notamment du commerce électronique, des dispositions améliorant la transparence et l'information vis-à-vis des usagers des plateformes permettront d'améliorer le niveau de protection des échanges.

Il s'agit, notamment, de garantir une exigence de transparence à l'égard des usagers sur les conditions de référencement des offres de vente, achat, prêt, et échanges et sur leurs droits et obligations.

Le projet de loi introduit donc dans le code de la consommation une définition des opérateurs de plateforme en ligne en fonction de leur activité. L'objectif poursuivi est, à l'instar, de ce qui a été adopté dans le cadre de l'article 134 de la loi du 6 août 2015 et de l'article L. 111-5 du code de la consommation sur les sites comparateurs inséré par la loi du 17 mars 2014 relative à la consommation, de mieux informer le consommateur avant qu'il effectue son choix d'achat de biens ou de prestation de services.

Seules les activités consistant à référencer, classer des contenus, des biens ou services proposés ou mis en ligne par des tiers ou de mettre en relation, par voie électronique, plusieurs parties en vue de la vente, de la fourniture d'un bien ou service, y compris non rémunérées, entrent dans le champ de la mesure. Cette limitation permet d'éviter d'imposer une obligation d'information à tous les sites Internet quel que soit leur champ d'activité.

En cohérence avec la disposition adoptée dans le cadre de la loi du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques, le projet de loi pose le principe d'une d'information loyale et transparente de l'opérateur de plateforme en ligne aux consommateurs sur les conditions générales d'utilisation du service, les modalités de référencement, de déréférencement et de classement des contenus.

La disposition prévoit, en outre, que les opérateurs de plateforme en ligne sont tenus de préciser l'existence ou non d'une relation contractuelle ou de liens capitalistiques avec les personnes référencées, ou l'existence d'une rémunération et son impact sur le classement, ce qui contribue à l'information loyale des consommateurs.

3. Options possibles et nécessité de légiférer

La consultation du Conseil national du numérique et les contributions de nombreux acteurs du numérique ont mis en évidence la nécessité d'améliorer la clarté et la loyauté de l'information des consommateurs.

La Fédération de la Vente à Distance (FEVAD) a mis en place, il y a plusieurs années, une charte de bonnes pratiques pour le commerce en ligne. Mais cet outil non contraignant et n'est pas applicable à toutes les entreprises intervenant sur Internet. Les contrôles menés par la DGCCRF, qui se sont accrus avec l'essor du commerce en ligne et de l'économie collaborative, confirment les limites de l'information des consommateurs sur les plateformes numériques.

Il apparaît donc nécessaire d'inscrire la mesure dans l'ordre juridique national.

En l'espèce, cette mesure vient compléter les dispositions du code de la consommation relatives aux sites comparateurs, aux places de marché et aux sites œuvrant dans le champ de l'économie collaborative qui sont soumis à une obligation d'information transparente et loyale.

4. Analyse des impacts des dispositions envisagées

4.1 Impact pour les consommateurs/particuliers

Les utilisateurs des sites des opérateurs de plateforme en ligne telles que définies par le projet de loi disposeront d'une information claire et transparente sur le classement des offres. Ils seront informés sur les modalités de référencement et déréférencement des annonces.

Ils disposeront en outre d'informations précises sur les conditions générales d'utilisation des sites et critères transparents de classement des offres notamment lorsque ces placements d'offres font l'objet d'une rémunération.

4.2 Impact pour les entreprises

Le projet de texte implique que les opérateurs de plateforme en ligne modifient l'ergonomie de leurs sites en ligne afin que les informations auxquelles elles sont tenues puissent y apparaitre de manière claire et lisible.

4.3 Impact pour les administrations et impacts budgétaires

La mise en œuvre de la mesure appellera des contrôles par les services habilités par le code de la consommation, donc ceux de la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes. Elle entraînera vraisemblablement la création d'un contentieux administratif spécifique lié aux recours formés à l'encontre des décisions d'amendes administratives prises par la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes, en cas de non-respect des obligations mises à la charge des professionnels. Cette nouvelle disposition engendrera nécessairement une mobilisation des services et des moyens supplémentaires ou une réorientation des priorités.

4.4 Impact sur l'ordre juridique interne/communautaire

Cette mesure introduit dans le code de la consommation des dispositions participant à l'amélioration du niveau d'information précontractuelle du consommateur. Elle s'inscrit dans la réflexion menée par la Commission européenne dans le cadre de l'agenda numérique qui s'intéresse notamment au rôle des plateformes, à la transparence et la loyauté des informations communiquées par ces plateformes à leurs utilisateurs.

5. Consultations menées :

Les entreprises du secteur ont été consultées sur ce projet de texte.
Le Conseil national de la consommation a également été consulté.

6. Outre-mer

L'article 46 du projet de loi rend l'article 22 applicable à Wallis et Futuna. L'article 47 modifie en conséquence le code de la consommation (nouvel article L. 116-2).

Article 23
Loyauté et régulation des plateformes

Cet article a pour finalité d'instituer la mise en œuvre d'une autorégulation des plateformes dont l'activité dépasse un seuil de nombre de connexions et de permettre à l'autorité administrative compétente de disposer d'éléments probants permettant un contrôle pertinent de l'activité de ces plateformes au regard de leurs obligations de loyauté et de transparence.

Il s'agit donc, au-delà des obligations inscrites dans le code de la consommation et définies à l'article 22, d'encourager les principales plateformes, dont l'impact sur l'économie et le pouvoir de marché sont très forts, à formaliser et mettre en œuvre de bonnes pratiques en matière de relations commerciales, à destination des consommateurs (afin de leur permettre de bénéficier d'une information claire et loyale) comme à destination des entreprises ayant des relations contractuelles avec les plateformes (afin de veiller à l'équilibre des conditions contractuelles).

1. <u>État des lieux</u>

Les principales plateformes en ligne, qui correspondent à des services variés (moteur de recherche, place de marché, plateforme d'intermédiation par exemple dans le domaine de l'économie collaborative) se caractérisent par un fort pouvoir de marché, renforcé par des effets de réseau très importants (« winner takes all »). Cette concentration se retrouve aussi bien du côté des consommateurs (par exemple le moteur de recherche de Google dispose d'une part de marché supérieure à 90% en Europe) que du côté des professionnels (annonceurs, etc.) ayant des relations commerciales avec les plateformes (par exemple, dans le domaine de la réservation hôtelière, différentes études suggèrent que les trois quarts des hôtels en France seraient référencés sur le site Booking.com, les réservations par cette agence en ligne représentant 30% de leur chiffre d'affaires). La loyauté de ces grandes plateformes dans leurs relations avec les consommateurs comme avec les entreprises revêt donc des enjeux économiques tout particuliers.

De manière générale, le projet de loi prévoit que toute plateforme en ligne est tenue de délivrer une information loyale, claire et transparente aux utilisateurs.

Il convient d'encourager les principales plateformes (notamment au regard de leur audience ou part de marché) à aller plus loin et de renforcer la transparence en permettant à leurs utilisateurs de mieux comprendre leurs conditions commerciales, et le cas échéant de mieux les comparer. Or, en l'état de la réglementation, les plateformes et notamment celles dont l'audience est importante, ne sont pas fédérées : ceci conduit à la mise en œuvre de pratiques distinctes, qui pourraient faire l'objet d'une mise en commun afin d'évaluer de manière précise la manière dont celles-ci mettent en œuvre leur obligation de loyauté et de transparence.

Il n'existe à ce jour aucune instance spécifique ni lieux d'échanges entre les plateformes les plus importantes et les principales parties prenantes, qui conduirait à développer pour l'ensemble du secteur des bonnes pratiques et permettre aux autorités publiques de contrôler plus aisément ces entreprises.

2. Description des objectifs poursuivis

Pour assurer la pleine effectivité de la mise en œuvre des principes de loyauté et de transparence, la mesure consiste à demander aux plateformes dont l'audience est importante à définir des bonnes pratiques et des indicateurs de référence et à rendre publique, périodiquement, l'évaluation de leurs propres pratiques. L'établissement d'indicateurs de performance et l'évaluation de leur application doivent permettre aux utilisateurs de disposer d'éléments améliorant leur confiance envers cette nouvelle économie numérique.

L'article prévoit, par ailleurs, pour réserver la mesure aux principales plateformes, qu'un décret fixera le seuil de connexions au-delà duquel les plateformes en ligne seront soumises à ces obligations. Ces bonnes pratiques pourront toutefois servir également de référence aux plateformes de plus petite envergure.

Afin de répondre aux attentes des parties prenantes et de rechercher une harmonisation des bonnes pratiques, des indicateurs et des informations transmises (et d'en faciliter la comparaison), il est souhaitable de prévoir une concertation entre les plateformes visées par cette mesure, ainsi qu'avec les parties prenantes.

Afin de disposer d'une concertation efficace et éviter l'écueil d'une collusion entre les acteurs les plus importants du secteur, les modalités d'organisation de cette concertation seront fixées par les pouvoirs publics. Les pouvoirs publics, les organisations professionnelles, les associations de consommateurs ou d'utilisateurs et les personnalités qualifiées y participeront. L'instance de concertation pourra s'appuyer sur des commissions consultatives existantes, notamment le Conseil national de la consommation et le Conseil national du numérique.

L'élaboration et la diffusion de bonnes pratiques, la détermination d'indicateurs pertinents de performance permettront également aux pouvoirs publics de mieux appréhender cette économie et de procéder si besoin à des enquêtes.

La disposition prévoit par ailleurs que l'autorité administrative compétente peut si elle l'estime nécessaire publier la liste des plateformes non vertueuses ne respectant par leur obligation et demander toutes informations utiles. Il s'agit par-là de compléter la possibilité de mener les enquêtes et de permettre à l'autorité administrative compétente de veiller à la bonne efficacité de la concertation et des initiatives des plateformes.

3. Options possibles et nécessité de légiférer

L'autorégulation des plateformes aurait pu être prise en charge par les acteurs professionnels eux-mêmes (de type labellisation ou charte de bonnes pratiques). Pour autant, en dépit des échanges récurrents sur cette question depuis plusieurs années, aucune initiative n'a véritablement germé pour progresser collectivement sur les principes de loyauté et d'auto-régulation.

Il est apparu plus adapté de formaliser et structurer, dans la loi, l'action attendue des plateformes.

Par ailleurs, la disposition prévoyant la possibilité pour l'autorité administrative compétente numérique de publier la liste des entreprises non vertueuses impose de légiférer tout comme le

principe d'une publication des indicateurs et de l'évaluation à la charge des professionnels concernés.

4. Analyse des impacts des dispositions envisagées

4.1 Impact pour les consommateurs/particuliers

Les utilisateurs des plateformes telles que définies par le projet de loi disposeront d'une information sur les pratiques exercées par les plateformes en ligne. Le projet de loi prévoit en effet une diffusion publique des indicateurs de performance.

4.2 Impact pour les entreprises

Le projet de texte porte sur les principales plateformes, au-delà d'un seuil de connexions. L'objectif est de viser, par ce moyen, une à quelques dizaines de plateformes structurantes pour l'économie française.

Pour ces plateformes, le projet de loi implique que les plateformes acceptent de participer loyalement et en toute transparence à l'élaboration des indicateurs de suivi de performance et d'évaluer périodiquement leurs pratiques.

4.3 Impact pour les administrations et impacts budgétaires

Ces nouvelles missions nécessitent la mobilisation de moyens humains complémentaires au-delà des attributions de contrôle déjà existantes. En effet, l'autorégulation et son contrôle par l'administration avec l'éventuelle publication de la liste des entreprises non respectueuses des principes de loyauté et de transparence est une nouvelle mission.

4.4 Impact sur l'ordre juridique interne/communautaire

Cette mesure introduit dans le droit français des dispositions visant à déterminer des indicateurs de performance et de résultats des plateformes en ligne en termes de respect du principe d'une information loyale, claire et transparente. L'élaboration des indicateurs viendra alimenter l'évolution en cours au sein de l'Union européenne, notamment l'action menée par la Commission dans le cadre de sa stratégie pour le marché numérique. En effet, la Commission européenne a lancé en septembre 2015 une enquête qui devrait aboutir à d'éventuelles propositions visant à modifier le fonctionnement et l'encadrement des plateformes en ligne.

5. Textes d'application et Outre-mer

Un décret fixera le seuil du nombre de connexions et les modalités d'application du projet d'article L.111-5-2 du code de la consommation.

L'article 46 du projet de loi rend l'article 23 applicable à Wallis et Futuna. L'article 47 modifie en conséquence le code de la consommation (nouvel article L. 116-2).

Section 4
Information des consommateurs

Article 24
Information des consommateurs sur les avis en ligne

Le projet de loi fixe une obligation d'information loyale sur la qualité des avis publiés sur l'internet et renforce l'information des consommateurs concernant les débits proposés dans les contrats.

1. État des lieux

La question de la fiabilité des avis en ligne revêt un enjeu clair tant pour le consommateur que pour les entreprises présentes sur internet. Si imposer une vérification systématique des avis serait de nature à créer une contrainte technique et matérielle excessive pour certains sites internet et à remettre en cause la diversité des sources d'information pour les consommateurs, il n'en demeure pas moins que la confiance du consommateur dans les avis en ligne, et plus largement dans le commerce électronique, doit être protégée.

En France, il existe, en parallèle, depuis juillet 2013, une norme AFNOR portant sur les processus de collecte, modération et restitution des avis en ligne de consommateurs mais celle-ci est d'application volontaire. 43 organisations ont participé à l'élaboration de la norme. Dans le dispositif prévu pour la vérification des avis déposés, l'ambiguïté qui existe entre les notions d'acte d'achat et d'expérience de consommation démontre les difficultés à transcrire de manière générale un système permettant de procéder à la vérification des avis mis en ligne. En outre, le respect de ce dispositif normatif par les professionnels volontaires ne leur permet pas pour autant d'alléguer sur la vérification des avis déposés sur leur site puisque la norme ne fait que certifier un processus.

Au 30 août 2015, 15 entreprises sont certifiées par l'AFNOR sur le fondement de cette norme : 12 d'entre elles sur la base de l'intégralité du processus de contrôle (collecte, modération et restitution) et 3 uniquement sur la partie modération des avis.
Néanmoins, les professionnels peuvent, sans faire mention de certification, préciser que leur processus de contrôle est conforme à la norme. Dans ce cas, elles engagent leur responsabilité, la norme n'étant pas certifiée.

En 2014, sur 118 établissements contrôlés, la DGCCRF a prononcé 15 avertissements, et dressé 6 procès-verbaux. La qualification majoritairement retenue est la pratique commerciale trompeuse.

2. Description des objectifs poursuivis

Le projet de loi introduit dans le code de la consommation une disposition imposant aux sites internet mettant en ligne des avis d'indiquer, de manière explicite, si leur publication a fait l'objet d'un processus de vérification, qu'il soit interne ou externe. Elle précise que, si le site procède à des vérifications, il est tenu d'en préciser clairement les principales modalités et de mettre ces informations à disposition des consommateurs de manière préalable. La mise en place de ce dispositif permettra ainsi au consommateur d'évaluer, par lui-même, le degré de

confiance qu'il sera à même d'accorder aux avis disponibles sur le site et, par extension, au site internet qui les publie. Placer ainsi le consommateur en position d'arbitre apparaît de nature à responsabiliser les responsables de site web dans la mise en ligne des avis et à favoriser un assainissement des pratiques existantes.

Le succès du commerce électronique repose sur deux postulats complémentaires : la sécurité de ce secteur assurée par les professionnels et la confiance accordée par les consommateurs en corollaire. Dans le cadre de ce dernier postulat, la question des avis en ligne tient une place de plus en plus prépondérante. En décembre 2014, l'étude de l'IFOP sur l'impact de l'e-réputation sur le processus d'achat montre que le Web est devenu un vecteur d'information incontournable pour les consommateurs puisque plus de 80% des internautes déclare avoir recours à internet pour se renseigner avant d'acheter un produit. Dans ce cadre, 88% des consommateurs consultent les avis en ligne avant de procéder à l'achat sur internet ou en magasin et 85 % d'entre eux indiquent avoir été dissuadés de faire un achat suite à la lecture d'avis négatifs sur des blogs, forums ou sites des consommateurs. Parallèlement, 75 % des français estiment que certains des avis sont faux.

3. Options possibles et nécessité de légiférer

Le projet de loi vient compléter les dispositions du code de la consommation relatives aux sites comparateurs, aux marketplaces et aux sites œuvrant dans le champ de l'économie collaborative qui sont soumis à une obligation d'information transparente et loyale. Compte tenu du principe d'harmonisation maximale fixée par la directive 2000/31/CE du 8 juin 2000 relative à certains aspects techniques des services de la société de l'information et notamment du commerce électronique, il n'est pas envisagé d'imposer une vérification systématique des avis par les professionnels qui les mettent en ligne. Il s'agit essentiellement d'informer les internautes que les avis en ligne qu'ils consultent ont fait ou non l'objet d'une vérification et la nature de celle-ci, afin de leur permettre de déterminer le degré de confiance qu'ils leur accordent dans le cadre de leur décision d'achat.

4. Analyse des impacts des dispositions envisagées

4.1 Impact pour les consommateurs/particuliers

Le baromètre 2015 ACSEL-CDC de la Confiance des Français dans le Numérique montre que, parmi les consommateurs interrogés, 89% d'entre eux ont recours aux sites de vente en ligne mais parallèlement, seulement 43% d'entre eux font confiance à ces commerçant en ligne, chiffre qui est en baisse par rapport aux statistiques publiés en 2013.

Les dispositions de l'article 24 permettront aux consommateurs de disposer d'une information claire et transparente sur la vérification des avis, de nature à augmenter le degré de confiance qu'ils sont susceptibles d'accorder au site de commerce en ligne qu'ils consultent.

Les consommateurs qui consultent ces avis n'ont pas toujours conscience que leur vérification n'est pas effectuée systématiquement par le site qui les publie. Les plateformes qui feront cette démarche devront, si elles communiquent sur ces vérifications, en préciser les caractéristiques principales et cela permettra ainsi aux consommateurs d'avoir une vision plus objective de l'information qui leur est délivrée.

4.2 Impact pour les entreprises

La question des avis en ligne dépasse la seule notion de commerce en ligne et s'intègre clairement dans la problématique de l'e-réputation. Ce concept agrège à l'espace numérique les questions d'identité et de notoriété. De nos jours, la « voix » de l'entreprise n'est plus unique et doit composer avec celles d'utilisateurs de mieux en mieux informés, de consommateurs de plus en plus experts et qui bénéficient d'un préjugé de confiance supérieur à celui dont elle bénéficie. Des avis positifs de consommateurs sont des relais puissant du discours commercial de l'entreprise ; à l'opposé, des avis négatifs de consommateurs, un « bad buzz », sont de nature à avoir un impact négatif dans la décision d'achat de clients potentiels.

Dans cette perspective, le dispositif prévu à l'article 24 implique que les sites publiant des avis en ligne, à titre principal ou accessoire, communiquent sur la vérification des avis postés par les consommateurs, que cette vérification soit réalisée en interne par l'entreprise ou externalisée auprès de prestataires spécialisés. Dans le même temps, les professionnels n'effectuant aucune démarche de vérification des avis publiés sur leur plateforme devront également mettre en place une information systématique sur leur site web.

L'obligation inscrite à l'article 24 permet de prendre en compte l'importance et la confiance qu'accordent les consommateurs aux avis de leurs pairs publiés en ligne et a vocation à encourager les professionnels du numérique soucieux de leur e-réputation, à mettre en place un système de vérification des avis en ligne et d'en informer les consommateurs. Pour les professionnels ayant déjà mis en place un système de vérification, les modalités mises en œuvre devront apparaître sur leur site, ce qui impliquera donc une modification de l'ergonomie de celui-ci.

4.3 Impact sur l'ordre juridique interne/communautaire

Cette mesure introduit dans le code de la consommation des dispositions participant à l'amélioration du niveau d'information précontractuelle du consommateur. Elle s'inscrit dans la réflexion menée par la Commission européenne dans le cadre de l'agenda numérique qui s'intéresse notamment au rôle des plateformes et à la transparence et la loyauté des informations communiquées à leurs utilisateurs.

5. Consultations menées

Ont été consultés sur ce projet d'article le Conseil National du Numérique ainsi que le groupe de travail auteur de la norme AFNOR NF Z74-501 pour fiabiliser le traitement des avis en ligne de consommateurs.

6. Textes d'application et Outre-mer

Un décret fixera les modalités d'application des mesures prévues par le présent article.

L'article 46 du projet de loi rend l'article 24 applicable à Wallis et Futuna. L'article 47 modifie le code de la consommation (nouvel article L. 116-2).

Article 25
Information des consommateurs sur les débits

Le projet de loi renforce l'information des consommateurs concernant les débits proposés dans les contrats.

1. État des lieux

L'information des consommateurs en matière de débits de connexion, proposés aujourd'hui dans les contrats, est définie à l'article L. 121-83 du code de la consommation. Les discussions dans le cadre européen du marché unique des télécommunications a fait apparaître un besoin de précision de ces informations.

2. Description des objectifs poursuivis

Ce projet d'article complète les dispositions du code de la consommation par des obligations relatives à l'information contractuelle des consommateurs sur les débits fixes et mobiles. Cette disposition permet une mise en en cohérence avec le règlement européen « marché unique des communications électroniques » et améliore ainsi la lisibilité du droit.

3. Options possibles et nécessité de légiférer

S'agissant des obligations d'information du consommateur, Ces dernières sont prévues par la proposition de règlement « marché unique des communications électroniques » qui visent à renforcer la transparence sur les pratiques de gestion de trafic, sur la qualité de l'accès à internet complètent le cadre européen issu de la directive 2002/22/CE du 7 mars 2002 modifiée dite « directive service universel » en matière d'information contractuelle des utilisateurs de services de communications électroniques transposé à l'article L. 121-83 du code de la consommation. Elles ont donc vocation à être transcrites dans ce même article, afin d'améliorer la lisibilité du droit.

4. Analyse des impacts des dispositions

Le renforcement de l'information des utilisateurs de services de communications électroniques poursuit les efforts déjà engagés par le Gouvernement pour améliorer l'information des consommateurs sur les débits offerts par les services de communications électroniques dont l'arrêté du 3 décembre 2013 relatif à l'information préalable du consommateur sur les caractéristiques techniques des offres d'accès à l'internet en situation fixe filaire constitue une première étape.

L'inscription à l'article L. 121-83 du code de la consommation de ces nouvelles obligations de transparence contractuelle permettra par ailleurs, si nécessaire, d'en préciser les modalités de mise en œuvre par la simple modification de l'arrêté d'application prévu au dernier alinéa de l'article L. 121-83 (arrêté du 16 mars 2006 relatif aux contrats de services de communications électroniques).

Une fois la loi adoptée, le Gouvernement sera en mesure d'adapter si besoin l'arrêté de 2006 en concertation avec les opérateurs et les associations de consommateurs

5. Consultations menées

Cet article a été soumis pour avis à l'ARCEP, en application de l'article L. 36-5 du code des postes et des communications électroniques, et à la Commission supérieure du service publique des postes et des communications électroniques, en application de l'article L. 125 du même code.

Chapitre II

Protection de la vie privée en ligne

La confiance dans le numérique ne peut durablement prospérer sans de solides protections en faveur de la vie privée et du respect des données à caractère personnel des usagers. Les évolutions constatées montrent à la fois un caractère de plus en plus intrusif des techniques et services numériques, et une préoccupation croissante des citoyens sur cette nouvelle frontière à inventer entre « vie en ligne » et « vie privée ».

Section 1
Protection des données à caractère personnel

La diffusion massive des technologies numériques dans la vie des Français fait apparaître de nouveaux défis pour le respect de certaines de nos valeurs, en particulier le droit au respect de la vie privée. La multiplication des fichiers publics et privés, la diffusion accrue des données à caractère personnel et la sophistication croissante des traitements sont l'un des plus visibles et des plus sensibles de ces défis.

Sur ces questions, la France dispose d'une législation ancienne et robuste aux évolutions technologiques avec la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

L'ampleur des collectes de données ainsi que plusieurs affaires récentes mettent néanmoins en exergue la nécessité d'un cadre renforcé pour la protection des données à caractère personnel.

Pour établir un environnement de confiance dans l'utilisation des outils numériques, le Gouvernement souhaite renforcer les droits des personnes vis-à-vis des fichiers contenant leurs données personnelles, et accorder des pouvoirs plus importants à la Commission nationale de l'informatique et des libertés (CNIL). Ces évolutions interviendront prioritairement à travers le règlement européen sur la protection des données personnelles, actuellement en cours de discussion et sur lequel les négociations devraient aboutir prochainement. La France promeut aussi au niveau européen, le renforcement des pouvoirs du « Comité Européen de la Protection des Données » (CEPD), instance regroupant les 28 autorités de protection des données européennes.

Toutefois, des évolutions sont également envisageables au plan national, en cohérence avec le projet de règlement. C'est l'objet des articles 26 à 33 du projet de loi.

Article 26
Libre disposition de ses données à caractère personnel

Le projet de loi énonce le principe général de la libre disposition de ses données personnelles.

1. **État des lieux**

Le droit de la protection des données personnelles est né, dans les années 1970, du développement de l'informatique. Il s'est d'abord formé dans le cadre national, avant d'être reconnu au plan européen et international (directive 95/46/CE, convention n° 108 du Conseil de l'Europe…).

Les textes correspondants reconnaissent aux personnes des droits sur les données qui les concernent, qu'il s'agisse de droits portant sur la constitution des fichiers (droit d'opposition, droit d'information, droit d'accès…) ou de droits relatifs à l'utilisation des données en vue de prendre des décisions.

L'accroissement considérable des usages et de la circulation des données personnelles liés au développement du numérique et la perte de contrôle des individus qui en résulte ont conduit certains à proposer d'inscrire ces droits dans un droit plus général de chacun à contrôler l'utilisation de ses données personnelles, plus précis que le droit au respect de la vie privée dans lequel s'inscrit déjà la protection des données personnelles.

Les principes posés par la loi relative à l'informatique, aux fichiers et aux libertés sont restés pertinents : opposition, accès, et rectification. Toutefois, ces instruments classiques souffrent d'ineffectivité compte tenu de la montée en puissance des services numériques fondés sur l'exploitation des données. Les individus se plaignent des difficultés pour faire valoir leurs droits face aux grands services collecteurs de données. Cette ineffectivité du droit s'illustre notamment par des conditions générales d'utilisation (CGU) longues, éparses et ambigües, ainsi qu'une forte opacité sur le sort des données collectées.

2. **Description des objectifs poursuivis**

Pour assurer la pleine effectivité des droits à opposition, accès et rectification affirmés par la loi de 1978, il convient de les asseoir sur un nouveau fondement, pour les renforcer et permettre, par exemple, aux individus de faire valoir leurs droits tout au long de la vie de la donnée, après sa collecte initiale.

Le principe de libre disposition de ses données personnelles a été dégagé par la Cour constitutionnelle allemande en 1983. Cette liberté, qualifiée d' « *autodétermination informationnelle* », est caractérisé par la Cour comme « *le pouvoir de l'individu de décider lui-même [...] quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui* ».

L'introduction dans la législation française du droit, pour toute personne, de « décider et de contrôler les usages qui sont faits de ses données à caractère personnel la concernant, dans les conditions et limites fixées par la loi informatique et libertés » vise à renouveler le sens donné à la protection des données à caractère personnel.

Il s'agit de passer d'une posture uniquement défensive, de protection des données personnelles à une posture plus offensive de maîtrise, de contrôle et plus encore de capacité pour l'utilisateur à mobiliser et utiliser ses données pour ses propres finalités. La consécration du principe de libre disposition de ses données vise en particulier à accompagner un nouveau paradigme : au-delà de la seule protection de leur vie privée, les individus cherchent à maîtriser leur vie en ligne.

Dans un environnement numérique caractérisé par d'importantes asymétries de pouvoir, ce droit à la libre disposition implique qu'ils puissent avoir accès à ces données, qu'ils puissent les lire, les modifier, les effacer, choisir ce qu'ils veulent en faire ; mais aussi qu'ils puissent décider des services qui y ont accès. Certes, la simple proclamation du principe de libre disposition de ses données ne suffira pas à le rendre effectif. Une consécration forte du principe permettra néanmoins de donner à un sens nouveau à la nécessaire transformation des instruments de protection des données : protection, maîtrise, usages. Dans une autre perspective, il s'agit de fournir à la fois au juge et au régulateur un nouveau fondement pour son action.

Selon l'étude annuelle du Conseil d'État de 2014 *« le numérique et les droits fondamentaux »,* quatre avantages sont à en attendre :

- donner un sens au droit à la protection des données personnelles : comme l'indique le Conseil d'État, *« il s'agit de donner à l'individu les moyens de demeurer libre de conduire son existence, dans une société où le numérique prend une place croissante, qui l'amène à laisser, de plus en plus souvent, trace de ses données personnelles »* ;
- donner un contenu positif au droit à la protection des données personnelles, qui peut, autrement, être perçu comme défensif ;
- marquer l'enjeu que représente pour les libertés publiques, la protection des données à caractère personnelle ;
- formuler un objectif ambitieux, qui *«* [joue] *un rôle d'aiguillon, tant pour les pouvoirs publics que pour les individus ».*

3. Options possibles et nécessité de légiférer

Comme il vient d'être indiqué, pour assurer la pleine effectivité des droits à opposition, accès, rectification et effacement affirmés par la loi de 1978, il convient de les asseoir sur un nouveau fondement, pour les renforcer et permettre, par exemple, aux individus de faire valoir leurs droits tout au long de la vie de la donnée.

Le Conseil d'État, dans son étude annuelle de 2014[65] précisait qu'il n'était pas souhaitable d'ajouter le droit à l'autodétermination informationnelle à la liste des droits déjà reconnus par

[65] « *Le numérique et les droits fondamentaux* », pages 264 à 269.

les textes existants. Ce droit doit s'entendre comme donnant sens à tous ces droits, « *qui tendent à le garantir et doivent être interprétés et mis en œuvre à la lumière de cette finalité.* »

Choix du support législatif

Trois supports peuvent a priori être envisagés pour l'inscription dans le droit national du principe de libre disposition de ses données personnelles :

- une disposition autonome, non codifiée, du projet de loi pour une République numérique ;
- le code civil ;
- la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le recours à une disposition autonome, non codifiée, ne pose pas de difficulté particulière mais n'est évidemment pas optimal du point de vue de la lisibilité et de l'intelligibilité du droit.

L'inscription de ce principe à l'article 9 du code civil serait plus solennelle et présenterait également l'avantage de rattacher le droit à libre disposition de ses données à la protection de la vie privée, comme l'a fait la jurisprudence lorsqu'elle s'est prononcée sur la protection des données à caractère personnel en se fondant sur l'alinéa 1er de l'article 9 du code civil.

La Cour de cassation a ainsi récemment jugé aux visas des articles 9 et 1382 du code civil que « *le choix d'une personne physique comme mot-clé destiné à faciliter le référencement par les moteurs de recherche sur internet des pages qui le supportent n'est pas fautif lorsqu'il n'est associé à aucune autre donnée personnelle, et ne le devient, le cas échéant, que lorsqu'est répréhensible le contenu de la page à laquelle de mot-clé est associé* » [66].

La modification de l'article 9 du code civil présenterait cependant l'inconvénient de donner une importance particulière au droit à la libre disposition de ses données personnelles à l'intérieur du droit au respect de la vie privée, alors même que le premier n'est qu'une des facettes du second.

La loi n° 78-17 du 6 janvier 1978 « informatique et libertés » constitue également un support pertinent pour le principe de libre disposition de ses données personnelles, en raison de son objet même mais aussi parce qu'il s'agit du texte fondateur du droit de la protection des données personnelles. Ainsi, une modification du chapitre II de la loi « informatique et libertés » apparaît comme une approche pertinente.

4. Analyse des impacts des dispositions envisagées

4.1 Compatibilité avec le droit de l'Union Européenne

Le principe de libre disposition de ses données personnelle n'est pas explicitement abordé par le projet de règlement européen, mais le texte du projet de loi ne pose pas de difficulté au regard du projet de règlement.

[66] Cour de cassation, 1ère chambre civile, 10 septembre 2014, n° 13-12.464.

4.2 Impact juridique

Comme le Conseil d'État le rappelait dans son rapport précité un débat existe sur la question de donner à ce droit à la protection des données personnelles un caractère patrimonial ou non.

Accorder un caractère patrimonial à ce droit à l'autodétermination informationnel poserait deux problèmes majeurs.

- Tout d'abord, sauf pour les personnes d'une particulière richesse ou notoriété, la valeur des données personnelles d'un individu est très limitée, de l'ordre de quelques centimes d'euros. C'est le très grand nombre de données traitées qui confèrent leur valeur aux bases manipulées par les acteurs du numérique. Ainsi, le rapport de forces entre l'individu, consommateur isolé et l'entreprise, resterait marqué par un déséquilibre structurel.

- En outre, la reconnaissance du droit de propriété de l'individu sur ses données pourrait poser des difficultés juridiques pour les pouvoirs publics. Ainsi, par exemple, les limites apportées par la loi du 6 janvier 1978 concernant le traitement des données personnelles devraient être justifiées au regard de l'atteinte au droit de propriété en tenant compte des jurisprudences de la Cour Européenne des droits de l'homme et du Conseil Constitutionnel. Reconnaître un droit de propriété de l'individu impliquerait en réalité de renoncer largement à la logique de protection.

Cette analyse est à l'origine du choix fait d'envisager la protection des données personnelles comme un droit à l'autodétermination. Le principe de libre disposition est ainsi considéré comme un droit attaché à la personne.

Une consécration forte du principe permettra de donner un sens nouveau à la nécessaire transformation des instruments de protection des données : protection, maîtrise, usages.
Il convient, à ce titre, de remarquer que la disposition envisagée indique que la protection des données personnelles se fera dans les conditions fixées par la loi informatique et liberté. »

5. Consultations menées

La CNIL, consultée, souligne que le droit de libre disposition de ses données *« renforce positivement les principes déjà proclamés à l'article 1er en renforçant la capacité de l'individu à maîtriser les usages qui sont faits de ses données à caractère personnel ».*

La libre disposition de ses données a fait l'objet d'une étude approfondie dans le cadre de l'étude annuelle 2014 du Conseil d'État qui portait sur le numérique et les droits fondamentaux.

L'affirmation d'un principe de libre disposition de ses données personnelles est également une proposition phare du Conseil national du numérique (CNN).

6. Textes d'application et outre-mer

En application de son article 72, la loi « informatique et libertés » est applicable en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises, en Nouvelle-Calédonie et à Mayotte.

L'article 46 du projet de loi rend les modifications apportées à la loi « informatique et libertés » par l'article 26 applicables dans ces territoires.

Article 27
Droit à l'information sur la durée de conservation des catégories de données traitées

1. État des lieux

La loi « informatique et libertés » décrit, dans son chapitre V, les obligations incombant aux responsables de traitements et les droits des personnes dont les données personnelles font l'objet d'un traitement. Est notamment prévue à son article 32 le droit à l'information portant notamment sur la finalité du traitement auquel les données sont destinées.

2. Description des objectifs poursuivis

Le projet de loi vise à compléter l'article 32 de la « loi informatique et libertés » afin d'ajouter que la *« durée de conservation des catégories de données traitées »* fait explicitement partie du périmètre des informations sur lesquelles le droit d'information évoqué supra s'applique.

3. Options possibles et nécessité de légiférer

L'article 32 de la loi « informatique et libertés » définit la liste des obligations des responsables de traitement en matière d'information des personnes auprès desquelles des informations à caractère personnel sont recueillies. Tout ajout à cette liste ne peut donc se faire que par voie législative.

4. Analyse des impacts des dispositions envisagées

Les modifications proposées permettront de renforcer l'information faite aux citoyens sur la durée de conservation de leurs données
La mesure prévue à l'article 27 du projet de loi est essentiellement sans impact (financier ou autre) pour les responsables de traitement qui n'auront qu'à compléter l'information qu'ils réalisent déjà en vertu de l'article 32 de la loi « informatique et libertés ».

5. Consultations menées

La Commission nationale de l'informatique et des libertés a été consultée.

6. Outre-mer

En application de son article 72, la loi « informatique et libertés » est applicable en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises, en Nouvelle-Calédonie et à Mayotte.

L'article 46 du projet de loi rend les modifications apportées à la loi « informatique et libertés » par l'article 27 applicable dans ces territoires.

Article 28
Exercice en ligne des droits relatifs aux données personnelles

1. État des lieux

La loi « informatique et libertés » décrit, dans son chapitre V, les obligations incombant aux responsables de traitements et les droits des personnes dont les données personnelles font l'objet d'un traitement.

Sont notamment prévus :

- une information portant notamment sur la finalité du traitement auquel les données sont destinées (article 32) ;
- un droit d'opposition, pour motifs légitimes, à ce que des données personnelles fassent l'objet d'un traitement (article 38) ;
- un droit d'information permettant notamment d'obtenir des informations sur le traitement lui-même ou les transferts de données à caractère personnel envisagés à destination d'un ÉtatÉtat non membre de la Communauté européenne (article 39) ;
- un droit d'accès et de rectification des données (article 40).

La plupart des responsables de traitement permettent d'exercer ces droits directement via un formulaire en ligne ou via contact par courriel mais cette pratique n'est aujourd'hui pas encore systématique, la loi n'interdisant pas par exemple, le recours à une procédure papier.

2. Objectifs poursuivis

L'article 28 du projet de loi vise à imposer que, dès lors que le responsable du traitement considéré dispose d'un site internet, l'exercice des droits prévus au chapitre V de la loi « informatique et libertés » puisse être exercés par voie électronique.

Cette disposition est destinée à garantir que l'exercice des droits puisse se faire de manière simple et la plus ergonomique possible. Outre l'intérêt évident pour les citoyens en matière d'exercice de leur droit, le recours à de telle pratique est susceptible de constituer un facteur de réductions de coût et de simplification pour les responsables de traitements.

3. Options possibles et nécessité de légiférer

L'obligation de mise en place d'un moyen électronique d'exercice des droits des personnes appelle également nécessairement une modification législative dans la mesure où elle modifie les modalités de satisfaction d'une exigence légale.

Cette nouvelle modalité devra s'articuler avec l'ordonnance n° 2005-1516 du 8 décembre 2005 relatives aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

4. Analyse des impacts des dispositions envisagées

Les modifications proposées permettront de faciliter et de simplifier l'exercice par les citoyens de leurs droits vis-à-vis des responsables de traitements de données à caractère personnel. Elles concourent ainsi à la réalisation de l'objectif indiqué à l'article 26.

La mesure prévue à l'article 28 du projet de loi peut nécessiter, pour les responsables de traitement qui n'en disposent pas déjà, la mise en œuvre d'un dispositif en ligne d'exercice des droits. D'une part, il peut être remarqué que la plupart des responsables de traitement disposent d'ores et déjà d'un mécanisme en ligne permettant l'exercice des droits. Pour une large majorité des responsables de traitement la mesure sera donc sans impact financier.

La mesure prévoit en outre que l'obligation de mise en œuvre d'un dispositif en ligne ne s'applique qu'aux responsables de traitement disposant d'un site web. Pour de tels responsables de traitement, le surcoût d'ajout du dispositif restera extrêmement marginal, l'infrastructure numérique pouvant servir de support étant déjà en place et pourra même constituer un facteur de réduction de coûts pour le responsable de traitement en remplaçant un processus papier par un processus électronique (coûts marginaux moindres).

5. Consultations menées

La Commission nationale de l'informatique et des libertés a été consultée sur cette disposition.

6. Outre-mer

En application de son article 72, la loi « informatique et libertés » est applicable en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises, en Nouvelle-Calédonie et à Mayotte.

L'article 46 du projet de loi rend les modifications apportées à la loi « informatique et libertés » par l'article 28 applicables dans ces territoires.

Article 29
Missions de la Commission nationale de l'informatique et des libertés (CNIL)

1. État des lieux

La Commission nationale de l'informatique et des libertés est l'autorité nationale de protection des données à caractère personnel. L'article 11 de la loi « informatique et libertés » définit ses missions, qui sont aujourd'hui au nombre de quatre :

- informer les personnes concernées et tous les responsables de traitements de leurs droits et obligations ;
- veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi ;
- émettre des avis sur les règles professionnelles et délivrer des labels ;
- se tenir informée de l'évolution des technologies de l'information.

2. Description des objectifs poursuivis

En vue de moderniser les compétences de la CNIL et de les adapter au développement du numérique, l'article 29 du projet de loi :

- assigne à la CNIL la mission de promouvoir l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données (2° f) de l'article 29) ;
- multiplie les cas de saisine pour avis de la CNIL (1° ° de l'article 29) ;
- confie à la CNIL le soin de conduire une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques (2° e) de l'article 29).

2.1 Promotion des technologies protectrices de la vie privée :

Le développement de technologies de nature à renforcer la maitrise par les personnes de leurs données personnelles est un des axes clef d'une amélioration de la protection des données sur Internet (et s'inscrit notamment dans l'approche « *privacy by design* » dans laquelle la protection de la vie privée est prise en compte dès le début de la conception du produit ou du service). Le champ des technologies concernées comprend par exemple les outils de paramétrage du traçage des données personnelles ou les outils de visualisation et de gestion des données personnelles détenues par des tiers. Ce sont également les technologies de chiffrement des données.

Compte tenu de l'importance que prennent ces technologies, une plus grande implication des pouvoirs publics dans leur élaboration est nécessaire. Il est logique de confier cette mission à la CNIL.

2.2 Consultation de la CNIL sur les projets de loi et de décret :

L'article 11 4° a) de la loi informatique et liberté prévoit que la CNIL est saisie pour avis sur *« tout projet de loi ou de décret relatif à la protection des données personnelles »*, ce qui conduit parfois à des interprétations divergentes, la création d'un fichier par la loi n'étant pas toujours regardée comme relevant de la « protection » des données personnelles au sens de cet article. L'article 29 du projet de loi opère donc une clarification de l'obligation de consultation de la CNIL en prévoyant que celle-ci doit être saisie de tout projet de loi ou de décret *« comportant des dispositions relatives à la protection des données à caractère personnel ou au traitement de telles données »*.

2.3 Réflexion sur les problèmes éthiques et les questions de sociétés soulevés par l'évolution des technologies numériques :

Les évolutions technologiques liées au numérique soulèvent nombre de questions d'ordre éthique et amènent la société à s'interroger sur les possibles atteintes à la dignité de la personne humaine et sur les valeurs dont il convient d'assurer le respect.

La transparence accrue des individus liée à la collecte massive de données et au développement du *big data* et les perspectives et enjeux du développement de la robotique et de l'humanité augmentée sont souvent cités comme des sujets sur lesquels un débat démocratique approfondi apparaît nécessaire.

Afin d'organiser ce débat, le Conseil d'État dans son rapport annuel consacré aux droits et libertés numériques, propose de créer une *« mission permanente d'animation de la délibération collective sur les enjeux éthiques liés au numérique »* (proposition n° 11). Inspiré du Conseil consultatif national d'éthique, ce comité aurait pour vocation d'organiser le dialogue entre les experts et la société sur les enjeux éthiques liés au numérique et d'associer cette dernière à la délibération sur ces sujets.

A priori, trois possibilités peuvent être envisagées pour l'organisation de cette mission :

- la création d'une instance *ad hoc* ;
- l'adossement au Conseil national du numérique ;
- l'adossement à la Commission nationale de l'informatique et des libertés.

La création d'une instance *ad hoc* est l'approche qui a été suivie dans le cas de la bioéthique, avec le Conseil consultatif national d'éthique. Elle ne semble cependant pas opportune dans le cas du numérique, d'abord parce qu'elle nécessite des moyens plus importants que l'adossement à une structure existante, mais, surtout, parce qu'il existe déjà dans le numérique des instances susceptibles d'accueillir cette mission.

Dans ce contexte, le choix de la CNIL, plutôt que du Conseil national du numérique, pour organiser la mission de réflexion sur les problèmes éthiques apparaît assez naturel en raison :

- de l'ancienneté de la commission et de la légitimité qu'elle a acquise avec le temps ;
- de son caractère d'autorité administrative indépendante, qui permettra de doter l'enceinte de réflexion des mêmes garanties d'indépendance ;
- des moyens dont dispose d'ores et déjà la commission.

3. Options possibles et nécessité de légiférer

De façon générale, la Commission nationale de l'informatique et des libertés dispose de compétences d'attribution qui sont fixées par la loi. Une évolution de ses attributions requiert donc une modification législative.

4. Analyse des impacts des dispositions envisagées

Impact sur la CNIL : compte-tenu des quelques ressources qui pourraient être dégagées par l'évolution des missions suite à l'adoption à venir du règlement européen sur les données personnelles, la CNIL peut assumer ces missions à moyens constants.

5. Consultations menées

La CNIL a été consultée sur cette disposition.

6. Outre-mer

En application de son article 72, la loi « informatique et libertés » est applicable en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises, en Nouvelle-Calédonie et à Mayotte.

L'article 46 du projet de loi rend les modifications apportées à la loi « informatique et libertés » par l'article 29 applicables dans ces territoires.

Article 30
Certificats de conformité

La confiance des entreprises à développer leurs activités et offres numériques est également conditionnée à la sécurité juridique qui s'y attache : le cadre législatif doit fournir des outils concrets afin de permettre aux entreprises désireuses par exemple de développer des usages innovants, de bénéficier d'un cadre juridique sécurisant et stable.

Le projet de loi crée ainsi un nouvel outil, « le certificat de conformité », destiné à assurer les entreprises d'une sécurité juridique pour leurs processus d'anonymisation.

1. État des lieux

Le cadre actuel de la protection des données personnelles repose sur des principes forts et sur un contrôle formel préalable important (déclaration préalable du traitement), mais pour lesquels les procédures de contrôle et les sanctions sont peu dissuasives[67].

Le projet de règlement européen prévoit une suppression du contrôle formel *ex ante* (déclaration) des traitements, la responsabilité de l'application des principes et des règles en matière de protection des données reposant dorénavant avant tout sur les responsables de traitement eux-mêmes. Pour les aider, différents mécanismes sont prévus :

- *privacy by design*, études d'impact et documentation des traitements réalisés ;
- désignation de personnes responsables de la protection des données dans l'entreprise ;
- mise en place de codes de conduite, de mécanismes de certification et de labels.

Le projet de loi, à travers l'article 37-1 qu'il insère dans la loi du 6 janvier 1978, s'inscrit dans cette démarche, en prévoyant la possibilité pour les responsables de traitement d'obtenir des certificats de conformité pour les processus d'anonymisation des données à caractère personnel.

2. Description des objectifs poursuivis

Le projet de loi a pour objectif de renforcer la sécurité des responsables de traitements, en particulier des entreprises qui mettent en œuvre ou projettent de mettre en œuvre de nouveaux services impliquant des traitements de données à caractère personnel.

3. Options possibles et nécessité de légiférer

Une option possible aurait été la mise en place d'un rescrit en matière de données personnelles. Un rescrit serait en effet un instrument adapté pour renforcer la sécurité juridique des porteurs de projets. Dans le cadre d'un rescrit, un responsable de traitement pourrait solliciter une prise de position de la CNIL sur la licéité de son traitement et la réponse

[67] En France, la loi informatique et libertés prévoit des sanctions maximales de 150 000 €.

apportée par la commission lui serait opposable, à condition que le responsable de traitement ait communiqué toutes les informations nécessaires.

La mise en place d'un véritable rescrit dans le domaine des données à caractère personnel se heurte cependant à des difficultés considérables.

D'abord, pour être utile, un tel rescrit devrait être simple ; en effet, le besoin de sécurité juridique concerne surtout les traitements « nouveaux », qui sont le plus souvent mis en œuvre par des start-ups du numérique. Or, ces entreprises ne disposent pas de ressources nécessaires pour suivre une procédure lourde de rescrit. Cependant, un rescrit très simple à obtenir provoquerait nécessairement un « appel d'air » (la CNIL reçoit chaque année plusieurs milliers de déclaration) et déboucherait inévitablement sur un engorgement des services de la commission.

Ensuite, le rescrit serait accordé au vu du traitement mis en œuvre, ou prévu, au moment où la demande est effectuée. Or les traitements de données personnelles, notamment ceux mis en œuvre par les start-ups, évoluent rapidement. Dans ce contexte, il y a un fort risque qu'une procédure de rescrit, à l'opposé de son objectif, augmente en réalité l'insécurité juridique, d'une part pour les responsables de traitement (qui pourront se croire protégés par le rescrit alors que celui-ci ne couvrira plus les traitements qu'ils mettent en œuvre) et, d'autre part, pour la CNIL (qui pourrait avoir des difficultés à sanctionner des traitements non-conformes mais pour lesquels elle aura délivré un rescrit au vu d'un état antérieur).

Compte tenu de ces difficultés, la piste du rescrit a été écartée, au profit d'un certificat de conformité de portée plus réduite puisque limitée aux processus d'anonymisation des données.

4. Analyse des impacts des dispositions envisagées

Cette disposition doit permettre d'améliorer la prise en compte par les entreprises des principes institués par la loi informatique et libertés ainsi que par la présente loi, et ainsi de diminuer leur risque de sanction.

5. Consultations menées

La CNIL a été consultée.

6. Outre-mer

En application de son article 72, la loi « informatique et libertés » est applicable en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises, en Nouvelle-Calédonie et à Mayotte.

L'article 46 du projet de loi rend les modifications apportées à la loi « informatique et libertés » par l'article 30 applicables dans ces territoires.

Article 31 et 32
Droit à l'oubli pour les mineurs et mort numérique

Le numérique est aujourd'hui omniprésent dans l'univers des enfants et des adolescents : là aussi, l'impératif de protection et de sécurité est plus qu'ailleurs une exigence sociale forte. Le projet de loi entend renforcer la protection des mineurs sur Internet.

Le projet de loi prévoit ainsi pour les mineurs une procédure accélérée en terme de « droit à l'oubli » renforcé.

Le projet de loi énonce également de nouvelles règles permettant aux usagers de définir, de leur vivant, les consignes à adopter, après leur disparition, à propos de leurs données personnelles mises en ligne.

1. État des lieux

1.1 Droit à l'oubli

De façon générale, le « droit à l'oubli » désigne la possibilité pour les individus d'obtenir la suppression d'information les concernant publiées sur Internet (droit à l'effacement) ou le déréférencement de ces informations par les moteurs de recherche (droit au déréférencement).

En Europe, l'arrêt « Google Spain » de la Cour de Justice de l'Union européenne, largement commenté, a consacré un « droit au déréférencement ». Cette construction jurisprudentielle est prolongée par le projet de règlement européen sur la protection des données à caractère personnel, en cours de discussion, qui prévoit la mise en place d'un véritable droit à l'effacement des données dans certaines circonstances.

La problématique du « droit à l'oubli » concerne toute personne mais se présente de manière spécifique dans le cas des personnes mineures. En effet, bien qu'ils soient souvent familiarisés très jeunes avec l'utilisation des technologies numériques (notion de « digital natives »), les mineurs n'ont souvent pas la maturité nécessaire pour apprécier les répercussions à moyen et long terme des informations qu'ils communiquent ou publient sur Internet. Par ailleurs, l'expérimentation - y compris, aujourd'hui, l'expérimentation numérique - est une composante essentielle du développement de la personne, mais n'a de sens que si elle s'accompagne d'un « droit à l'erreur ». Or, l'Internet n'oublie jamais et ne corrige jamais.

Ceci a conduit un certain nombre d'observateurs à proposer l'établissement de règles spécifiques en matière de « droit à l'oubli » pour les mineurs et à certaines initiatives en ce sens, comme la loi spécifique adoptée par l'État de Californie en 2013 et entrée en application début 2015.

La loi du 6 janvier 1978 ne comporte aucune disposition propre aux mineurs, alors même que l'immense majorité d'entre eux utilise, entre autre, les réseaux sociaux, et que les questions de e-réputation sont régulièrement liées à des données mises en ligne avant l'âge de la majorité.

1.2 Mort numérique

Avec le développement de la « vie numérique », la question du devenir des données des personnes décédées commence à prendre de l'importance.

Différentes questions se posent en effet lorsqu'une personne décède : que devient le profil de cette personne sur les réseaux sociaux ? Les descendants et héritiers du défunt peuvent-ils accéder aux données de celui-ci stockées, par exemple pour conserver des souvenirs du défunt ? Que deviennent les « actifs numériques » (photos, livres électroniques, musique numérique...) du défunt ?
Force est de constater que les réponses à ces questions demeurent très partielles.
En effet, l'ouverture d'un compte de messagerie ou d'un compte sur un réseau social sur Internet confère à son titulaire des droits personnels. Il s'agit du droit au respect de la vie privée, qui comprend notamment le droit au secret des correspondances, et du droit à l'image. Les règles de la dévolution successorale ne sont pas applicables à ces droits qui n'ont pas une nature patrimoniale. Dès lors, dans le silence du contrat, les héritiers ne peuvent pas imposer aux gestionnaires des comptes de leur transmettre les données qu'ils contiennent.

Les fournisseurs de services de communication au public en ligne qui gèrent de nombreux comptes et sont régulièrement confrontés à la question de la « mort numérique » (sur Facebook, un profil sur cent serait celui d'une personne décédée) ont cependant commencé à apporter des réponses.

Ainsi, Facebook a annoncé la création d'une fonctionnalité « Legacy Contact », qui permet à un contact de confiance d'accéder au compte d'un utilisateur décédé pour transformer le profil en « mémorial » virtuel et, le cas échéant, récupérer les photos du profil et des archives des publications. C'est la suite d'un processus amorcé en 2009, date à laquelle un ingénieur de Facebook avait proposé la première fonctionnalité de « mémorial » après avoir été confronté au décès d'un proche.

D'autres services, comme celui de Google, offrent désormais la possibilité pour les vivants d'organiser le devenir de leurs données après leur mort.

En revanche, la législation concernant les données personnelles des personnes décédées reste embryonnaire.

Certains textes existent déjà notamment pour les comptes bancaires inactifs et les contrats d'assurance-vie en déshérence.

Par ailleurs, des possibilités d'accès à certaines informations concernant la personne décédée et de rectification de ces données ont été ouvertes aux ayant-droits par l'article L. 1110-4 du code de santé publique et par l'article 40 de la loi « informatique et libertés » - qui permet aux héritiers d'une personne décédée de demander l'actualisation des données à caractère personnel concernant la personne décédée afin de prendre en compte le décès[68] -, mais ces dispositions n'assurent pas un traitement systématique et global de la question.

---

[68] L'article 40 dispose *: « Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.*

Enfin, en son état actuel, le projet de règlement européen exclut les personnes décédées de son champ d'application.

2. Description des objectifs poursuivis

2.1 Droit à l'oubli

L'article 32 du projet de loi a pour objectif d'introduire au bénéfice des personnes mineures une procédure accélérée leur permettant d'obtenir, sur demande, dans des délais réduits, l'effacement, en ligne, de leurs données à caractère personnel. La disposition s'inscrit en conformité avec la mise en œuvre à venir du règlement européen, lequel consacre ce « droit à l'effacement ».

Ceci permettra ainsi d'exercer dans des délais rapides un « droit à l'oubli » protecteur de la vie privée des intéressés, qui sont les plus vulnérables dans l'univers numérique.

2.2 Mort numérique

Le projet de loi complète l'article 40 de la loi « informatique et libertés » en prévoyant la possibilité pour toute personne de formuler des directives (générales ou particulières) concernant le devenir de ses données personnelles à son décès.

Les directives générales sont enregistrées auprès d'un tiers de confiance numérique certifié par la CNIL et les directives particulières sont enregistrées auprès des responsables de traitements.

Ces directives « définissent la manière dont la personne entend que soient exercés après son décès les droits qu'elle détient » en application de la loi « informatique et libertés ». Elles ne créent donc pas de nouveaux droits pour les personnes vis-à-vis des responsables de traitement.

Les directives peuvent désigner une personne chargée de leur exécution ; à défaut de désignation, un ordre de priorité entre les héritiers est fixé.

Le projet de loi prévoit toutefois que les prestataires qui stockent des données sur l'internet sont tenus de transmettre les données d'une personne décédée à la personne que le défunt aura désignée préalablement.

Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent. »

L'article 100 du décret n° 2005-1309 du 20 octobre 2005 précise : *« Outre la justification de son identité, l'héritier d'une personne décédée qui souhaite la mise à jour des données concernant le défunt doit, lors de sa demande, apporter la preuve de sa qualité d'héritier par la production d'un acte de notoriété ou d'un livret de famille. »*

3. Options possibles et nécessité de légiférer

3.1 Droit à l'oubli

Seule la loi peut prévoir une procédure d'exception au bénéfice des mineurs et indiquer les délais impératifs à respecter dans ces cas.

3.2 Mort numérique

La question des données à caractère personnel des personnes décédées n'est pas abordée dans le projet de règlement européen. En l'absence d'initiative européenne, une alternative se présente :

- maintenir le statu quo, c'est-à-dire laisser le traitement de la question de la « mort numérique » entre les mains des fournisseurs de services de communication au public en ligne ;
- légiférer au niveau national.

Le maintien au statu quo n'est pas satisfaisant car il laisse perdurer les difficultés que rencontrent les ayant-droits d'une personne décédée pour accéder aux données et rend les réponses qui sont apportées au problème par trop dépendantes du modèle économique de fournisseurs de service.

L'approche retenue par le projet de loi vise essentiellement à faciliter :

- d'une part, l'expression des volontés du défunt ;
- d'autre part, l'action de ses ayant-droits dans le respect desdites volontés ;
- enfin, en l'absence de directives, la possibilité pour les héritiers d'exercer les droits du de cujus après son décès.

4. Analyse des impacts des dispositions envisagées

4.1 Droit à l'oubli

Compatibilité avec le droit de l'Union Européenne :

L'article 17 du projet de règlement européen[69] (droit à l'effacement et à l'oubli numérique) oblige le responsable du traitement à effacer dans les meilleurs délais, les données à caractère personnel, notamment en ce qui concerne les données à caractère personnel qui sont collectées lorsque la personne concernée a le statut d'enfant, dans un certain nombre de cas qu'il détermine.

Le projet de loi s'inscrit en pleine conformité avec le règlement européen à venir, dès lors qu'il fait explicitement référence aux conditions prévues par ce règlement.

[69] Orientation générale adoptée par le Conseil JAI (document 9565/15 du 11 juin 2015).

4.2 Mort numérique

Compatibilité avec le droit de l'Union Européenne : la question des données à caractère personnel des personnes décédées est explicitement exclue du projet de règlement européen.

Impact sur la CNIL : la CNIL devra certifier les « tiers de confiance numérique » auprès desquels les directives générales pourront être déposées.

Impact sur les responsables de traitement : les responsables de traitement devront créer une procédure permettant de recueillir les directives particulières des personnes. Ils devront également communiquer les données du défunt à la personne que celui-ci aura désignée, le cas échéant. Enfin, ils devront informer l'utilisateur du sort de ces données et permettre à ce dernier de choisir de communiquer ou non ses données à un tiers qu'il aura préalablement désigné.

5. Consultations menées

La CNIL a été consultée sur ces dispositions.

6. Textes d'application et Outre-mer

Un décret en Conseil d'État fixera les modalités d'application des mesures d'effacement des données mentionnées à l'article 32.

En application de son article 72, la loi « informatique et libertés » est applicable en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises, en Nouvelle-Calédonie et à Mayotte.

L'article 46 du projet de loi rend les modifications apportées à la loi « informatique et libertés » par les articles 31 et 32 applicables dans ces territoires.

Article 33
Procédure de sanction de la CNIL

Une politique efficace en faveur de la protection de la vie privée en ligne et des données personnelles se mesure aussi à l'aune des sanctions encourues en cas d'infractions. La crédibilité de la régulation est ici en jeu et le projet de loi entend renforcer le volet sanction de la législation en vigueur.

Le projet d'article renforce les pouvoirs et procédures de sanctions à la disposition de la CNIL.

1. **État des lieux**

La CNIL dispose d'un pouvoir de sanction dont les modalités d'exercice sont fixées par l'article 45 de la loi « informatique et libertés ».

La procédure retenue pour la CNIL, qui distingue les pouvoirs d'instruction (contrôle, mise en demeure, désignation d'un rapporteur pour saisine de la formation restreinte), relevant des pouvoirs propres du président, et les pouvoirs de sanction, relevant de la seule formation restreinte, ont été regardés par le Conseil d'État comme conformes aux exigences constitutionnelles par une décision de mars 2012. Cette procédure est d'ailleurs l'une des références dans les réflexions qui ont conduit à l'évolution des procédures devant d'autres autorités. Elle n'a donc pas vocation à évoluer sur un plan procédural.

En revanche des améliorations peuvent y être apportées afin de renforcer l'efficacité de la procédure.

Il est, par ailleurs, nécessaire de renforcer les sanctions prévues. Ce point est traité dans le cadre du projet de règlement européen en cours de négociation.

2. **Description des objectifs poursuivis**

Le projet de loi a pour objectif de renforcer l'efficacité et la crédibilité du processus répressif. Il s'agit d'un complément important à la responsabilisation accrue des responsables de traitement prévue par le projet de règlement européen.

Dans cette perspective, l'article 33 :

- permet à la CNIL de fixer le délai imparti à un responsable de traitement pour se mettre en conformité avec la loi à 24 heures en cas d'extrême urgence, au lieu de cinq jours au moins actuellement ;
- élargit le champ du référé judiciaire ;
- autorise la CNIL à prononcer une sanction pécuniaire sans mise en demeure préalable dans certaines circonstances ;
- autorise la CNIL à ordonner qu'une personne sanctionnée informe de cette sanction l'ensemble des personnes concernées.

3. Options possibles et nécessité de légiférer

3.1 Réduction du délai de mise en demeure à 24 heures en cas d'extrême urgence :

Actuellement, lorsqu'un traitement est mis en œuvre illégalement ou porte une atteinte grave à la vie privée, seule la formation restreinte peut ordonner la cessation de celui-ci, au terme d'une procédure de mise en demeure puis de sanction. Le président de la CNIL peut donc mettre en demeure un responsable de traitement de se mettre en conformité, tout en laissant « vivre » un traitement illégal pendant ce temps.

Il apparait donc utile que dans ce cas de figure et à condition de se trouver face à une situation d'extrême urgence, le délai de mise en demeure soit réduit à 24 heures.

3.2 Elargissement du champ du référé judiciaire :

La CNIL a aujourd'hui la possibilité de saisir le juge des référés, mais uniquement pour que soient mises en œuvre, sous astreinte, les « mesures de sécurité » nécessaires. Cela peut valoir, par exemple, en cas de « faille de sécurité » à combler. Mais la CNIL n'a pas la possibilité juridique, par exemple, de suspendre un traitement de données qui serait particulièrement risqué (ex : un traitement discriminatoire, ou qui révèlerait des données de santé couvertes par le secret médical). Il lui faut en effet engager une procédure répressive, consécutive à une mise en demeure. Il est donc proposé de supprimer les mots « de sécurité » pour que la CNIL puisse, de manière générale, saisir le juge des référés de toute demande tendant, notamment, à la suspension sans délai d'un traitement.

3.3 Possibilité de prononcer une sanction sans mise en demeure préalable :

Actuellement, lorsque la situation est particulièrement urgente ou que le manquement n'appelle plus de correction, le président de la CNIL peut décider de saisir directement la formation restreinte, sans mise en demeure préalable. Toutefois, cette formation ne peut alors prononcer qu'un avertissement, le cas échéant public, alors même qu'il s'agit souvent de cas graves mais limités dans le temps (comme, par exemple, une faille de sécurité ponctuelle qui n'appelle plus de mise en conformité – donc de mise en demeure – mais qui, pour autant, a effectivement causé un préjudice). Pour tenir compte de ces situations, le projet d'article ouvre donc la possibilité pour la formation restreinte de prononcer une sanction pécuniaire sans mise en demeure préalable *« lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure »*.

3.4 Publicité des sanctions auprès de chaque personne concernée :

La CNIL peut d'ores et déjà rendre publiques les sanctions qu'elle prononce. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne aux frais des personnes sanctionnées. Le projet d'article prévoit en outre que chaque personne concernée puisse être informée individuellement de l'existence de ces sanctions.

4. Analyse des impacts des dispositions envisagées

Le projet de règlement européen prévoit un renforcement des sanctions en cas de non-respect de ses dispositions mais ne comporte pas de disposition de procédure.

L'article 33 du projet de loi ne pose donc aucune difficulté au regard du projet de règlement. Au contraire, en améliorant l'efficacité et la crédibilité du pouvoir de sanction de la CNIL, il contribue à la réalisation des objectifs du règlement.

5. Consultations menées

La CNIL a été consultée sur ce projet d'article. Elle a estimé que l'article 33 *« permet une meilleure réactivité et efficacité des organes compétents de la Commission nationale de l'informatique et des libertés ».*

6. Outre-mer

En application de son article 72, la loi « informatique et libertés » est applicable en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises, en Nouvelle-Calédonie et à Mayotte.

L'article 46 du projet de loi rend les modifications apportées à la loi « informatique et libertés » par l'article 33 applicables dans ces territoires.

Section 2
Confidentialité des correspondances privées

Article 34
Respect des correspondances privées numériques

Le projet de loi réaffirme le principe du secret des correspondances, quel que soit la configuration technique du service de communication utilisé.

1. État des lieux

Le principe du secret des correspondances est le principe cardinal du droit des télécommunications. Le code des postes et des communications électroniques énonce clairement en son article L. 32-1 (5) que « *les opérateurs de communications électroniques sont tenus au secret des correspondances* ». A ce jour, la règle du secret des correspondances est ainsi directement rapportée au champ des opérateurs de services de communications électroniques.

Or, aujourd'hui, de nombreux services en ligne (services de téléphonie sur IP, réseaux sociaux, services de messagerie en ligne…) sont les supports de correspondances privées mais la plupart d'entre eux tendent à faire valoir que le code des postes et communications électroniques ne leur est pas applicable.

Des évènements récents montrent au surplus que certains services de correspondance privée en ligne offerts aux usagers français ne respectent pas en effet le secret des correspondances et ont occasionné des atteintes massives à l'intégrité de ces correspondances.

2. Description des objectifs poursuivis

Il convient de garantir l'application de la règle du secret des correspondances à toutes les correspondances privées, quel que soit le vecteur ou la technologie de communication utilisé. L'objectif est de lever la controverse en édictant clairement que l'ensemble des services de communication au public en ligne qui permettent d'échanger une correspondance privée sont astreints au respect du secret des correspondances. Il est précisé que le secret des correspondances couvre le contenu de la correspondance, l'identité des correspondants, ainsi que, le cas échéant l'intitulé du message et des documents joints à la correspondance.

Le projet d'article prévoit une exception pour les traitements qui ont pour fonction l'affichage, le tri ou l'acheminement de ces correspondances, la fourniture d'un service bénéficiant uniquement à l'utilisateur ou la détection de contenus non sollicités ou de programmes informatiques malveillants.

3. Options possibles et nécessité de légiférer

Compte tenu de la nature du dispositif envisagé, qui touche aux libertés publiques, le vecteur législatif est requis. Le dispositif devrait être intégré facilement à la partie législative du code des postes et des communications électroniques. Les compétences de contrôle de l'ARCEP permettront de s'assurer du respect et de l'effectivité du nouveau dispositif.

4. Analyse des impacts des dispositions envisagées

4.1 Impact sur les fournisseurs / coûts de mise en conformité :

Les fournisseurs des services en ligne (messagerie, téléphonie, réseaux sociaux …), offrant une fonctionnalité de service de correspondance privée, devront mettre en place les développements nécessaires pour se mettre en conformité avec la règle et présenter, le cas échéant, à l'autorité de contrôle compétente, les garanties appropriées.

4.2 Impact sur les conditions de concurrence :

L'application uniforme de la règle du secret des correspondances, que ce soit pour les opérateurs de communications électroniques ou les fournisseurs de services en ligne, produit un effet positif d'alignement des conditions de concurrence entre des acteurs qui sont effectivement la plupart du temps compétiteurs sur de mêmes segments de marchés.

4.3 Impact Confiance :

Le rappel catégorique par le législateur de la règle du secret des correspondances peut susciter un signal positif dans le mouvement croissant de défiance quant au respect de la vie privée dans les services numériques.

5. Consultations menées

Cet article a été soumis pour avis à l'ARCEP, en application de l'article L. 36-5 du code des postes et des communications électroniques, et à la Commission supérieure du service publique des postes et des communications électroniques, en application de l'article L. 125 du même code.

6. Outre-mer

L'article 46 du projet de loi rend l'article 34 applicable à Wallis et Futuna. L'article 47 (IV) modifie en conséquence l'article L. 32-3 du code des postes et des communications électroniques.

TITRE III

L'accès au numérique

Chapitre I^er^

Numérique et territoires

Section 1
Compétences et organisation

Article 35
Stratégie numérique des collectivités

1. **État des lieux**

Les schémas directeurs territoriaux d'aménagement numérique (SDTAN) ont été définis par la loi du 17 décembre 2009 relative à la lutte contre la fracture numérique.

Conformément à l'article L. 1425-2 du code général des collectivités territoriales, *« les schémas directeurs territoriaux d'aménagement numérique recensent les infrastructures et réseaux de communications électroniques existants, identifient les zones qu'ils desservent et présentent une stratégie de développement de ces réseaux, concernant prioritairement les réseaux à très haut débit fixe et mobile, y compris satellitaire, permettant d'assurer la couverture du territoire concerné. Ces schémas, qui ont une valeur indicative, visent à favoriser la cohérence des initiatives publiques et leur bonne articulation avec l'investissement privé (...) ».*

Un SDTAN correspond à un territoire sur lequel il est unique. Ce territoire doit recouvrir un ou plusieurs départements ou une région. Il a pour objectif de permettre aux différents acteurs, notamment aux collectivités, de définir une stratégie concertée de déploiement des réseaux sur le territoire concerné.

L'élaboration d'un SDTAN constitue un préalable à l'intervention d'une collectivité territoriale en faveur du déploiement du très haut débit sur son territoire.

La démarche des SDTAN a connu un grand succès et, au 15 octobre 2014, seuls cinq département français n'étaient pas concernés par un tel schéma directeur.

2. **Description des objectifs poursuivis**

Le projet de loi a pour objectif d'étendre au domaine des services numériques la démarche des SDTAN. Il s'agit d'inclure dans le SDTAN, une stratégie de développement usages et services numériques. Cette stratégie deviendra un volet à part entière du SDTAN.

Comme dans le cas des infrastructures numériques, couvertes par les SDTAN, une approche souple est nécessaire. En effet, le développement des services numériques n'est pas une compétence exclusive des collectivités territoriales, mais ressort également à l'initiative privée et à l'État. C'est pourquoi l'exercice de cette compétence est purement facultatif et l'élaboration donne lieu, le cas échéant, à une concertation.

De la même manière, le développement des services numériques n'est pas nécessairement du ressort d'un seul échelon de collectivités territoriales. Ainsi, le projet de loi prévoit que les schémas directeurs territoriaux des usages et services numériques peuvent être établis par les régions ou par les départements. Il n'exclut pas a priori que plusieurs schémas directeurs puissent concerner le même territoire, même si cette situation n'apparaît pas optimale en termes de stratégie de déploiement.

3. Nécessité de légiférer

Pour éviter la multiplication des schémas régionaux, il est proposé de compléter le code général des collectivités territoriales par un article L. 1425-3 qui organise ce nouveau volet du SDTAN. La définition des schémas directeurs territoriaux étant prévue par la loi, la modification de leur consistance doit se faire par la loi.

4. Analyse des impacts des dispositions envisagées

Le projet d'article a pour objectif d'améliorer la cohérence et la pertinence des choix faits en matière de politique de développement des services numériques dans les territoires. Il n'impose pas de contrainte particulière car la mise en place de la stratégie de développement des usages et services numériques est une faculté à la disposition des collectivités territoriales. Ces dernières demeurent libres de mettre en œuvre ou non ce schéma directeur et d'y affecter ou non les moyens nécessaires. Il convient également de noter que ces schémas directeurs territoriaux n'auront qu'une simple valeur indicative et visent essentiellement à favoriser la cohérence des initiatives publiques.

Le schéma directeur numérique des collectivités est avant tout un outil mis à disposition pour accompagner la montée en compétence numérique des collectivités, sans qu'il soit imposé à ces dernières d'obligation spécifique en la matière.

5. Consultations menées

Cet article a été soumis pour avis à l'ARCEP, en application de l'article L. 36-5 du code des postes et des communications électroniques, à la Commission supérieure du service publique des postes et des communications électroniques, en application de l'article L. 125 du même code, et au Conseil national d'évaluation des normes.

Article 36
Syndicats mixtes ouverts

1. État des lieux

Lancé au printemps 2013, le Plan France Très Haut Débit (PFTHD) a pour objectif la couverture de l'intégralité du territoire en très haut débit d'ici 2022 afin de garantir un accès à internet performant à l'ensemble des logements, des entreprises et des administrations. La priorité politique rappelée par le Président de la République lors du comité interministériel aux ruralités du 14 septembre 2015, invite à mobiliser tous les efforts possibles pour l'atteinte de ces objectifs. Or le dispositif actuel suscite des attentes supplémentaires, notamment s'agissant du rythme de lancement des projets de réseaux d'initiative publique, et de leur dimensionnement géographique.

2. Objectifs poursuivis

Pour inciter la mise en place de grands projets et garantir la cohérence des projets d'implantation des réseaux de communications électroniques à très haut débit sur l'ensemble du territoire de la République, la présente disposition favorise le regroupement de syndicats mixtes ouverts (SMO) et qui ont reçu, de la part des collectivités, la compétence pour développer un réseau de communications électroniques. Il s'agit en outre de permettre à des SMO, qui réalisent a posteriori, l'intérêt d'un regroupement à l'échelle supra-départementale, de permettre ce regroupement et donc de construire un projet de plus grande ampleur.

3. Options possibles et nécessité de légiférer

La disposition concernant le droit des collectivités territoriales, elle relève par nature du niveau législatif.

Deux options ont été envisagées, soit modifier l'article L. 5721-2 du code général des collectivités territoriales, soit l'article L. 1425-1 du même code qui traite spécifiquement des réseaux de communications électroniques. C'est cette dernière option qui a été retenue.

La nécessité de faire concorder les objectifs du PFTHD avec le regroupement de syndicat mixte ouvert a été prise en compte. De cette façon, de tels regroupements ne pourront avoir lieu que durant le plan et ne pourra pas être utilisé au-delà. Cette limitation permet de cadrer très strictement ce nouveau mécanisme dans le temps et évite la dilution du consentement des collectivités membres des syndicats mixtes.

4. Analyse des impacts des dispositions envisagées

Il s'agit d'un nouveau mécanisme offert au syndicat mixte ouvert. S'il décide une mise en œuvre, alors les moyens associés au SMO seront transférés vers le SMO désigné pour un regroupement. Il n'y a pas d'ajout de moyens financiers supplémentaires. Au surplus, le regroupement de SMO pourrait permettre aux collectivités de réaliser des économies d'échelle en partageant des coûts à une échelle supra-départementale. En définitive, cette option laisse entrevoir davantage de synergies que de coûts supplémentaires.

4. **Analyse des impacts des dispositions envisagées**

Deux dispositifs sont envisagés :

- d'une part, une obligation sur les services publics et les entreprises qui devront à terme pouvoir être joints par toute personne sourde ou malentendante, ce qui implique qu'ils se dotent en interne d'interprètes, ou bien qu'ils fassent appel, pour fournir ce service accessible, à un prestataire spécialisé. L'impact financier pour une autorité administrative ou une entreprise diffèrera selon leur taille, la volumétrie des appels à leur service téléphonique, etc. A titre d'exemple, une entreprise de relais téléphonique facture ses services, sur la base d'un forfait annuel illimité, entre 70€ pour une commune de moins de 2 000 habitants, un médecin, un boulanger et 15 000€ voire 20 000€ pour une grande entreprise ou un conseil départemental. A l'instar de ce qui se fait déjà en matière de mutualisation des services d'accueil téléphonique (ex. télé-secrétariat médical) les collectivités territoriales, comme les entreprises, pourront se regrouper et mutualiser les coûts en s'adressant à un même prestataire. Ces regroupements permettront ainsi de jouer à la baisse sur le montant annuel des abonnements et de diminuer l'impact financier de l'obligation sur les différentes collectivités
- d'autre part, une obligation pour les opérateurs de communications électroniques qui devront développer une offre commerciale accessible pour les services fixe et/ou mobile. Un décret précisera les contours minimaux de cette offre dont le tarif devra rester abordable.

La combinaison de ces deux dispositifs permettra d'assurer l'accessibilité des services téléphoniques aux personnes sourdes et malentendantes en complément des dispositifs existants. Les personnes sourdes et malentendantes s'appuient en effet déjà beaucoup sur les nouvelles technologies pour communiquer, notamment les SMS, la visiophonie, les mails, etc. Les progrès technologiques permettent par ailleurs d'espérer le développement de nouveaux outils dans les prochaines années facilitant l'autonomie des personnes déficientes auditives face au téléphone.

Compte tenu de l'absence des ressources en interprétariat et transcription nécessaires pour satisfaire à la mise en accessibilité immédiate des services téléphoniques visés et des délais nécessaires à la formation de personnels qualifiés, une entrée en vigueur différée pour l'application de ces dispositions est requise. Cette entrée en vigueur doit également intervenir de façon progressive, les entreprises les plus importantes devant fournir un service accessible les premières.

Selon l'étude menée par la société Orange Consulting chargée d'évaluer le besoin en matière d'accessibilité des services téléphoniques pour les personnes sourdes et malentendantes, ainsi que les différents scenarios de mise en œuvre envisageables, l'appropriation par les populations concernées sera progressive.

Le nombre d'utilisateurs de centre relais (tous usages confondus : appels personnels et professionnels) devrait atteindre **91 000 en dix ans**, répartis de la façon suivante :

- 54.000 pour le texte
- 34.000 pour la LSF

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

V

Table des matières

La protection des données de santé à caractère personnel
Pour la reconnaissance des droits du patient

Résumé

Les données personnelles sont omniprésentes sur internet et leur importance économique est croissante. Pour les services de la société de l'information tels que les moteurs de recherche, les réseaux sociaux ou les sites de vente en ligne, elles sont devenues indispensables. Ces services apparaissent comme essentiellement gratuits pour les utilisateurs mais ont en réalité un modèle économique particulier : la monétisation des données personnelles des utilisateurs, en échange d'un accès gratuit. Le texte originel de la loi du 6 janvier 1978, dite « Informatique et Libertés », est le texte de référence en matière de protection des données à caractère personnel et permet d'assurer une protection étendue des données. Fondée par le principe du droit à l'autodétermination, cette loi permet d'assurer un traitement des données à caractère personnel, dans le respect du droit à la vie privée. Néanmoins, la loi dite « Informatique et Libertés » originelle ne prenait pas en compte l'apparition des nouveaux traitements de données sensibles en dehors du domaine médical. La directive Européenne 95/46/CE fait un apport, notamment en matière de protection des données biométriques. Cependant, on assiste au développement de nouvelles technologies qui permettent la collecte d'un nouveau type de données personnelles se rattachant à une personne et permettant son identification. Celles-ci sortent du cadre réglementé du cabinet médical. Les nouvelles technologies de l'information font apparaître un nouveau type de données difficile à définir. Ces nouveaux types d'informations sur la santé, générées et collectées directement par la personne concernée, font également l'objet de nombreux travaux au niveau européen. En effet, le Parlement Européen et le Conseil de l'Europe ont voté un nouveau Règlement visant à renforcer le cadre juridique en matière de circulation et de protection des données à caractère personnel. Le renforcement de la protection des données personnelles et des données de santé fait également l'objet d'un projet de loi, présenté par la secrétaire au gouvernement A. Lemaire, qui vise à développer une « république numérique ». Ce projet a notamment pour objectif de renforcer certains principes fondamentaux comme le droit d'accès ou le droit à l'information. Il développe un nouveau concept comme « l'habeas corpus numérique » qui vise à renforcer les prérogatives de chaque utilisateur et à maîtriser davantage les données personnelles, notamment dans le domaine de la santé.

Summery

The protection of personal health data. In recognition of patient rights.

Personal data is omnipresent on the internet and their economic importance is growing. For the information society services such as search engines, social networks, or online shopping sites, they have become indispensable. These services appear as essentially free for users, but actually have a particular economic model: the monetization of personal data of users in exchange for free access. The new data processing necessity an original governance by law.