N° 579

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 23 janvier 2018.

AVIS

PRÉSENTÉ

AU NOM DE LA COMMISSION DES AFFAIRES SOCIALES SUR LE PROJET DE LOI *relatif à la* **protection** *des* **données personnelles**,

PAR MME ALBANE GAILLOT,

Députée.

Voir le numéro :

Assemblée nationale : **490**.

SOMMAIRE

—

Pages

AVANT PROPOS

La protection des données personnelles n'est pas une préoccupation nouvelle pour le législateur. En réaction à la mise en place de fichiers interconnectés à l'aide du numéro Insee, et à la suite de la commission « informatique et libertés » qui rédigea le rapport Tricot, fut adoptée la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Ses nombreuses dispositions permettent encore de protéger le citoyen mais nécessitent d'être adaptées pour tenir compte du développement du numérique et de la mondialisation des échanges de données permises par Internet.

Le projet de loi relatif aux données personnelles comporte un certain nombre de modifications consécutives à l'adoption du règlement européen de protection des données [(1)] (RGPD). Il tient également compte des marges de manœuvre que le RGPD accorde aux États membres pour renforcer le degré de protection ou, au contraire, alléger certaines contraintes. L'esprit du RGPD, c'est en même temps que la simplification des procédures, la responsabilisation des acteurs. C'est également la possibilité d'innover avec l'exploitation des données à l'aide des nouveaux outils numériques en même temps que la protection des droits accordés aux citoyens de l'Union. Il prend acte de l'élévation des données biométriques et génétiques au rang de données sensibles, au même titre que les données de santé. Pour ces catégories, le principe reste l'interdiction de traitement sauf dérogations strictement encadrées. Il précise les droits attachés à la protection des citoyens faisant l'objet des traitements de données personnelles. Surtout, la notion de données de santé fait l'objet d'une définition large, élevant le degré d'exigence des traitements de données qui ne relevait pas de ce périmètre jusqu'alors.

L'esprit du RGPD, dans lequel s'inscrit le projet de loi, vise à alléger les charges résultant des formalités préalables de déclaration ou d'autorisation de traitements de données personnelles. Le droit proposé vise à davantage responsabiliser les acteurs qui seront tenus de se conformer au cadre de référence élaboré avec l'autorité de régulation, de procéder à une analyse des risques d'atteinte aux droits fondamentaux et liberté et qui pourront faire l'objet d'un contrôle *a posteriori*. Le régime des sanctions est considérablement renforcé (jusqu'à 4 % du chiffre d'affaires s'agissant des amendes pécuniaires). Il est par ailleurs attendu une amélioration de la capacité de contrôle dans le cadre des actions coordonnées entre les autorités régulatrices au niveau européen. Enfin, le principe de l'application du droit de l'Union et de ses États est explicitement

(1) Règlement européen (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel qui constitue le cadre général de la protection des données.

prévu y compris pour les traitements opérés hors territoire de l'Union européenne pourvu qu'ils concernent un résident européen.

La commission s'est saisie pour avis des articles 7, 9 et 13 du projet de loi qui traite des données sensibles, du numéro d'inscription au répertoire (NIR) et des données de santé. Sur l'ensemble de ces points, le Gouvernement a entendu pleinement utiliser les marges de manœuvre offertes par le RGPD. S'agissant des donnés de santé, le défi consiste à combiner allégement des formalités préalables, maintien des distinctions de régime selon l'approche de la loi du 6 janvier 1978 [(1)] et confirmation du cadre juridique issue de la loi de modernisation de notre système de santé [(2)] pour les travaux de recherche.

Le projet de loi maintient l'équilibre actuel entre nécessaire protection des données de santé et recherche.

Suivant le mouvement opéré par le nouveau cadre européen, le traitement des données fera davantage l'objet de procédures allégées impliquant des déclarations de conformité à des cadres de référence, le régime d'autorisation demeurant l'exception.

Le cadre juridique des traitements de données de santé relatifs aux recherches, qui fait intervenir d'autres acteurs au côté de la CNIL, s'inscrit aussi dans ce même mouvement. Guichet unique des dossiers relatifs aux recherches n'impliquant pas les personnes humaines, l'Institut national des données de santé (INDS) voit son rôle évoluer vers davantage d'accompagnement des acteurs. Il pourra toujours se prononcer sur l'intérêt public des traitements aux fins de recherche sur saisine de la CNIL ou auto-saisine.

Afin de conforter une approche homogène de la notion d'intérêt public, le texte étend même cette faculté aux traitements dont les finalités ne sont pas définies (entrepôt de données).

Le projet de loi conforte les assouplissements de la loi de modernisation de notre système de santé (LMSS) s'agissant de l'appariement du NIR aux données de santé. Cette possibilité est importante pour le maintien de la qualité des travaux de recherche.

La modification du régime de décision de la CNIL (le silence vaut acceptation) permettra d'accélérer le traitement des demandes et de maintenir un haut niveau de recherche, et partant, d'innovation et de compétitivité.

Le texte présente plusieurs enjeux.

Le premier défi devra être relevé par les responsables de traitement. L'appropriation des normes et leurs impacts économiques ont été régulièrement

---

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

(2) Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

abordés au cours des auditions, confortant l'analyse du Conseil d'État dans son avis transmis au Gouvernement. Cet enjeu concerne aussi bien les organismes publics que privés qui ont attesté, en auditions, du caractère très anxiogène de ce nouveau cadre juridique. Investis d'une responsabilité d'autant plus importante que le régime de sanction est alourdi, les acteurs se situent en première ligne. Cette anxiété peut aussi se nourrir des confusions résultant des choix rédactionnels opérés par le Gouvernement. C'est particulièrement le cas de l'article 13 qui définit le cadre juridique des traitements portant sur des données de santé. Chacun des acteurs auditionnés, y compris l'INDS, a ainsi fait part de ses interrogations à la rapporteure.

Or, s'il allège les formalités, l'article 13 ne modifie en rien l'approche aujourd'hui retenue et n'opère pas de bouleversement majeur dans les procédures. Interrogés en audition, les services du ministère de la santé ont bien souligné qu'il n'est nullement question de procéder à un « *sur-encadrement* » des dispositifs. Cette souplesse nécessitera un important effort de pédagogie. Ce rapport s'y emploie modestement.

Le second défi concerne la CNIL. L'autorité de régulation a parfaitement anticipé les évolutions opérées par le règlement. Elle a élaboré une doctrine d'emploi conforme aux nouvelles exigences tout en opérant un basculement de ses services vers l'accompagnement des opérateurs publics et privés. Toutefois, les objectifs sous-tendus par la nouvelle logique de régulation nécessitent un renforcement des capacités opérationnelles tant pour l'accompagnement que pour le contrôle. Il est illusoire de penser que cet objectif ambitieux pourra être atteint à effectif constant. Il en va de la crédibilité de la réforme. La puissance publique doit prendre toute sa part pour faciliter la transformation vers un rôle d'accompagnateur et non plus simplement de contrôleur.

Le dernier défi concerne les acteurs de données qu'ils s'agissent des citoyens eux-mêmes (producteurs de données) ou des responsables de traitement.

Il concerne tout d'abord ceux qui seront appelés à participer aux traitements des données personnelles, qu'ils soient professionnels de santé, acteurs industriels, ou organismes de recherche. Le recueil du consentement, le droit à l'information, le droit de rectification, le droit à l'oubli, pour ne citer qu'eux, supposent, de leur part, une démarche éthique qui compte autant que la qualité des données recueillies, aussi bien lors de la collecte que lors du traitement et de l'analyse. Les données de santé requièrent une vigilance toute particulière. Aussi la rapporteure estime-t-elle nécessaire de conforter le régime de traitement des données de santé par le développement de labels ou de certifications attestant d'une démarche éthique, sous le contrôle de la CNIL.

Les citoyens, en leur qualité de producteurs de données, doivent, quant à eux, être particulièrement vigilants quant au consentement accordé à l'utilisation de leurs données personnelles, particulièrement leurs données de santé, et tout particulièrement dans un univers qui tend à se numériser entièrement. Le

consentement comme le fait de rendre publiques ses données, constituent, il faut le rappeler, une dérogation au régime de formalités devant la CNIL. Un ambitieux chantier de sensibilisation doit être entrepris. Le hiatus important entre la légitime volonté de protéger ses données personnelles et l'insouciance quant au consentement accordé dans les outils de la vie quotidienne pose question et engage notre responsabilité afin de créer un cadre juridique sécurisant et de développer une pédagogie adaptée à cet environnement en perpétuelle mutation. On voit ainsi des internautes publier des informations sur leur santé sur les réseaux sociaux… S'il peut résulter en un « clic » acceptant les conditions générales d'utilisation des plateformes numériques, le consentement n'en constitue pas moins un acte déterminant.

Enfin, ce texte s'inscrit dans un contexte de développement sans précédent des outils numériques. Le projet de loi n'a pas vocation à tout régler, son objectif étant limité à la mise en place du paquet européen des données personnelles. De nombreux angles morts subsistent. La rapporteure aimerait prendre date. Il importe que le législateur se saisisse de la prochaine révision des lois de bioéthique pour relever le défi de l'intelligence artificielle, de l'homme augmenté et préciser ses intentions quant au « droit des robots » ou quant au cadre juridique des données non personnelles. Ces nouveaux paramètres doivent être pris en considération, faute de quoi le législateur aura manqué à sa mission.

I. LES DÉFIS POSÉS PAR L'IRRUPTION DU NUMÉRIQUE

« *Quelque chose est en train de se passer* ». Par ces quelques mots, le Conseil d'État, dans son étude annuelle 2017 [(1)], résume l'immense défi auquel le continent européen, la France en particulier, est confronté.

Le texte examiné par le Parlement tient à la protection des données personnelles. Il s'inscrit dans un contexte bien plus vaste, celui du développement sans précédent du numérique, un bouleversement profond porté par l'émergence des géants américains du numérique (les fameux GAFA [(2)]), de la mine d'or représentée par les données personnelles, des possibilités croissante de stockage et du hiatus existant entre les approches juridiques américaine et européenne. L'emploi des technologies numériques a aussi modifié nos usages. Il s'est en effet diffusé dans tous les aspects de notre vie quotidienne qu'ils s'agissent des loisirs, des nouvelles formes de sociabilité, de l'information, des échanges ou du développement économique. Il génère également un nombre exponentiel de données. Le RGPD comme le projet de loi constituent une réponse appropriée à des enjeux.

A. LE NUMÉRIQUE REND SUPERFÉTATOIRE L'INTERMÉDIATION D'UN TIERS DE CONFIANCE

Le développement du numérique bouscule autant qu'il rend désuet la nécessité du recours à un tiers pour faciliter les transactions ou définir des règles communes. La confiance ne réside plus dans le caractère immuable des règles de droit, parfaitement incarnées dans la puissance publique, mais dans le codage appelé à faciliter les échanges sans crainte d'erreur humaine.

1. La promesse de la désintermédiation

La promesse portée par le numérique est celle de la désintermédiation ce qui ne va pas sans poser de question sur le rôle de l'État, et partant, le maintien de la culture juridique qui le fonde. Les pays de culture latine sont sans nul doute beaucoup plus concernés que les pays de culture anglo-saxonne pour lesquels le droit est fondé sur une relation de confiance : le contrat plutôt que la loi.

Cette désintermédiation est très perceptible si l'on s'attache quelque peu à l'apparition des plateformes numériques : « *l'ubérisation* » est autant une vision prométhéenne – celle de la libération des contraintes de l'entrepreneur postmoderne – qu'un repoussoir pour nombre de concitoyens en demande de protection.

---

(1) Conseil d'État, Étude annuelle 2017, « Puissance publique et plateformes numériques : accompagner l'« ubérisation » »*, 13 juillet 2017.*

(2) Google, Apple, Facebook et Amazon.

Le Conseil d'État a parfaitement décrit cette réalité.

Le numérique est la réalisation d'une promesse, parfois au prix de l'affranchissement des contraintes. Le téléchargement illicite interroge le droit d'auteur, l'économie collaborative (le *sharing*) interroge la propriété intellectuelle, l'autorégulation par les objets connectés bouscule la relation médecin-patient, la personnalisation des traitements et la possible sélection des risques peuvent écorner la solidarité entre bien portants et malades.

Cette liberté se nourrit de la désintermédiation qu'opèrent parfaitement les puissantes plateformes numériques qui font notre quotidien. Dans l'un de ses ouvrages [(1)], Olivier Iteanu se propose d'ailleurs de décrire « *la journée ordinaire d'Alice* » : consultation de l'agenda *Google* au réveil, prise en compte des dernières informations sur les réseaux sociaux (*Twitter*, *Instagram*, *Facebook*), commande d'un taxi *via Uber*, écoute de la musique avec *Napster*, appel téléphonique avec *Whatsapp*, et pour finir, la vision d'un film *via Netflix* et l'accueil du touriste franchement débarqué qui profitera d'une location de chambre réservée par le biais d'*Airbnb*…

Cette désintermédiation présente plusieurs caractéristiques qui sont résumées dans le rapport du Conseil d'État.

En mettant en relation la « multitude », les plateformes permettent à l'ensemble les individus d'interagir quelles que soient les échelles géographiques (locale, nationale, continentale ou mondiale), cette interaction pouvant être bilatérale ou multilatérale. Dans ce dernier cas, le téléchargement de vidéos sur Internet se fait en optimisant les données mises à disposition par plusieurs utilisateurs distincts.

La désintermédiation porte en elle une « *dynamique d'individualisation* » et la personnalisation des services qui sont apportés. Ce n'est plus le sachant qui est à la manœuvre mais l'utilisateur qui transmet l'information au profit de la collectivité *via* la plateforme qui opère le tri, procède à sa hiérarchisation avec l'aide de l'utilisateur-notateur et présente le produit à l'utilisateur en tenant compte de ses préférences : les trajets routiers en temps réel suggérés par *Waze* plutôt que « *Bison futé* » pour les vacanciers ou « *Sytadin* » pour les automobilistes franciliens.

La désintermédiation n'est pas dépourvue d'objectifs économiques car elle permet de « *tendre irrémédiablement* » vers le coût zéro, ainsi que le souligne le rapport du conseil d'État. L'absence d'intermédiaires, c'est aussi l'élimination des coûts de transaction : pas de frais d'acquisition de nouveaux clients et encore moins de coûts de collecte d'informations puisque celles-ci proviennent

(1) Olivier Itéanu, « Quand le digital défie l'État de droit *», Eyrolles, 2016.*

directement des utilisateurs. Luc Ferry l'a fort justement résumé dans son dernier essai [1].

La gratuité d'utilisation n'est tout d'abord qu'apparente puisque le modèle économique est basé sur les données fournies par l'utilisateur qui, elles, peuvent être cédées à un tiers. « *Si vous ne payez rien en apparence, c'est que « c'est vous le produit* » », souligne ainsi Luc Ferry rapportant la formule attribuée à Tim Cook le dirigeant d'Apple. Et le philosophe d'ajouter : « *En clair : s'ils ne vous font rien payer quand vous utilisez leurs services, c'est parce qu'ils collectent, grâce à vos navigations diverses, une infinité d'informations sur vous qui se revendent à des prix faramineux aux entreprises qui en tirent des enseignements précieux pour cibler leurs clients* ».

Dernière caractéristique des plateformes selon la présentation qu'en fait le Conseil d'État : la relation de confiance. C'est l'autorégulation par les utilisateurs qui constitue la pierre angulaire du système. L'évaluation ou la notation permettent ainsi de déterminer la qualité de la prestation de services. Cette relation de confiance est aussi renforcée par la mise à disposition d'informations personnalisées à l'utilisateur qui, en retour, sera amené à alimenter la plateforme avec ses propres informations.

2. « *Code is law* [2] » ou la technologie comme marque de confiance

Le recours à la technologie constitue le moyen le plus efficace d'instaurer une relation de confiance. Plusieurs moyens sont ainsi proposés.

a. L'algorithme et l'intelligence artificielle

Selon la définition qu'en donne le Larousse, l'algorithme consiste en un « *ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur* ». Le mot « algorithme » vient du nom du mathématicien persan Al Khwarizmi qui introduisit en Occident la numération décimale et enseigna les règles élémentaires des calculs s'y rapportant. La notion d'algorithme est donc historiquement liée aux manipulations numériques. Cette notion, et les applications qui en résultent, ne sont pas nouvelles. Toutefois, la puissance de calcul des ordinateurs permet aujourd'hui d'en faire une utilisation intensive pour orienter les décisions et opérer des choix.

La plateforme *Google* en fait une utilisation massive pour opérer le référencement des sites et des blogs via ses algorithmes *Panda* (qui sanctionne les sites de mauvaises qualités au contenu de faible valeur ajoutée), *Pingouin* (qui traque les sites internet utilisant des techniques frauduleuses pour influer sur le

---

(1) Luc Ferry, « La révolution transhumaniste, comment la technologie et l'uberisation vont bouleverser nos vie *», éditions Plon, 2016.*

(2) Le code est la loi.

référencement) ou *Colibri* (qui est censé garantir la pertinence des réponses à une question posée).

Ce que prévoit le projet de loi sur le recours aux algorithmes

Sur l'enjeu particulier des algorithmes, le règlement autorise le recours aux algorithmes tout en laissant une marge d'appréciation pour les États. Le projet de loi opère une évolution en ouvrant la possibilité pour l'administration de recourir à des décisions prises sur le fondement d'un algorithme, dans le seul champ des décisions administratives individuelles, à l'exception notable des données sensibles. L'étude d'impact du projet de loi précise la justification de cette évolution : le maintien de l'interdiction absolue « *ne permet pas de répondre aux évolutions de l'activité administrative qui a de plus en plus recours à des traitements algorithmiques, notamment pour les décisions de masse que la réglementation encadre précisément et dont l'édiction rapide permet la bonne délivrance du service public* ».

Comme le rappelle la commission nationale de l'informatique et des libertés (CNIL) dans sa dernière synthèse du débat public portant sur l'intelligence artificielle [(1)], celle peut se définir, comme « *la science qui consiste à faire faire aux machines ce que l'homme ferait moyennant une certaine intelligence* », selon les termes employés par le mathématicien américain Marvin Lee Minsky. Elle comprend deux sous-ensembles :

– le *machine learning* (apprentissage automatique) qui est une technologie permettant aux ordinateurs d'apprendre sans avoir été programmés explicitement à cet effet. Plutôt que de décomposer en instructions la tâche à accomplir, l'homme entraîne le système en lui fournissant un certain nombre de données à partir desquelles la machine établira elle-même les opérations à effectuer pour accomplir la tâche. L'écriture prédictive des *smartphones* en constitue un exemple concret.

– le *deep learning* (apprentissage profond) constitue la plus récente étape du *machine learning*. La technique fonctionne comme un réseau de neurones. Un algorithme de *deep learning* parcourt ainsi un certain nombre d'exemples identifiés comme semblables pour en déterminer des caractéristiques communes et utiles pour la reconnaissance. Il pourra s'agir de plusieurs photos d'une même personne ou d'un même objet dans différents contextes. L'exemple le plus évocateur est la détection par la voiture autonome Google de son environnement pour détecter les obstacles : les éviter et s'arrêter au bon comment.

b. Le développement des objets connectés

Les objets connectés constituent une deuxième modalité de l'orientation de nos décisions en fournissant un service personnalisé. Le *Smartphone* en premier lieu, la montre connectée désormais, le réfrigérateur connecté aussi, … les

(1) CNIL, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle *», synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une république numérique, décembre 2017.*

possibilités offertes par la multiplication de ces objets sont si importantes que l'Union européenne a investi près de 200 millions d'euros sur la recherche comme le souligne le rapport du conseil d'État précité.

Ce développement se traduit notamment par le *Quantified self*, la mesure de la performance qui contribue, quelque peu, à la production sociale de normes de comportements comme le nombre de pas à réaliser quotidiennement.

C'est le domaine de la santé qui sera le plus concerné par le développement des objets connectés comme le souligne le cahier innovation et prospective élaboré par la CNIL (référence n° 2) :

« *Le domaine de la santé au sens le plus large sera naturellement le marché phare de l'internet des objets : dans son rapport «* Disruptive Technologies *» de mai 2013, le McKinsey Global Institute considère que le secteur de la santé portera seul entre un tiers et la moitié de l'impact économique annuel mondial de l'internet des objets en 2025 (qu'il évalue par ailleurs au chiffre mirobolant de 2 700 à 6 200 milliards de dollars par an…), essentiellement par la réduction des coûts du traitement des maladies chroniques*. »

c. La blockchain

La *blockchain* (chaîne de blocs) constitue enfin l'exemple le plus abouti de la désintermédiation. Elle repose sur une technologie permettant de garantir l'anonymat « *en certifiant de manière absolue l'intégralité des échanges, sans recours à un tiers de confiance* » (1). Elle consiste en un registre des échanges décentralisé, car partagé entre plusieurs acteurs, et répartis entre plusieurs blocs de données, reliés entre eux par le biais d'un cryptage. *Bitcoin* en constitue l'exemple le plus emblématique mais d'autres applications ont recours à cette technologie. Le Ghana a mis en place un cadastre au moyen de cette technologie alors que « *près de 90 % des terres rurales ne sont pas enregistrées sur des bases de données et, où de nombreux citadins n'ont pas encore d'adresse officielle* » (2).

B. DES ENJEUX JURIDIQUES ET ÉTHIQUES IMPORTANTS

Chacun de ces développements pose plusieurs questions afférentes à l'utilisation des nouveaux outils numériques et à leurs conséquences sur notre édifice juridique

1. La relation de confiance face au numérique

a. Le codage et la confiance dans la neutralité du Net

L'algorithme et l'intelligence artificielle posent les enjeux de la neutralité du Net et de l'orientation des décisions.

---

(1) Conseil d'État, op. cité.

(2) Conseil d'État, op. cité.

Un code n'est pas neutre et est écrit en fonction d'objectifs précis. Il comporte des biais et peut concourir à des discriminations et des exclusions.

Son utilisation est de nature à soulever d'importantes questions éthiques, d'autant plus qu'un individu n'est pas toujours en mesure d'en comprendre le fonctionnement. Le rapport du Conseil d'État met ainsi en lumière une affaire jugée par la Cour suprême de l'État du Wisconsin au sujet d'application COMPAS [(1)]. La juridiction devrait notamment de se prononcer sur le droit à un procès équitable, le juge de première instance ayant fondé sa décision d'incarcération sur le recours à un algorithme visant à produire un score de risque de récidive. La Cour a conclu qu'il était licite de recourir à ce traitement non pour déterminer le degré de la peine mais pour concourir à la prise de décision en corroborant l'appréciation du juge.

La synthèse de la CNIL rapporte également les propos tenus par M. Philippe Besse, professeur de mathématiques et de statistique à l'université de Toulouse, à l'occasion d'un débat organisé à Toulouse. Ce dernier souligne l'inégalité des patients devant la médecine personnalisée, les bases de données utilisées étant largement biaisées : 96 % des échantillons proviennent d'ancêtres européens, l'âge et le genre n'étant pas en reste : les bases de données concernent essentiellement les personnes âgées et les porteurs de chromosome X. Ces biais ont suffi à apporter la conclusion suivante : « *si vous êtes une femme d'origine africaine et jeune, je ne pense pas que la médecine personnalisée vous concerne* » [(2)].

Enfin, dernier enjeu et non des moindres, les algorithmes « *augmenteraient la propension à ne fréquenter que des objets, des personnes, des opinions, des cultures conformes à leurs propres goûts et à rejeter l'inconnu* » [(3)]. C'est toute la question de l'enfermement algorithmique qui est aussi en jeu comme le rappelle la citation de Benjamin Loveluck [(4)] mise en lumière dans l'ouvrage d'Olivier Iteanu : « *L'un des risques encourus […] est un enfermement de l'individu dans les catégories ainsi bâties, ce qui a pour corollaire de diminuer l'exposition à des informations diverses, voire d'orienter fortement les choix individuels et attenter ainsi à l'autonomie individuelle* ». Les spécialistes sont cependant divisés sur cette question, certains soulignant l'importance de la diversité des informations apportées par internet, d'autres s'interrogeant, comme la CNIL, sur la qualité et la vitalité du débat public faute d'exposition à l'altérité.

---

(1) Correctionnal Offender Management Profile for Alternative Sanction.

(2) CNIL, op. cité.

(3) CNIL, op. cité.

(4) Docteur en études politiques (EHESS) et chercheur post-doctoral au Centre d'études et de recherches de sciences administratives et politiques.

b. Les objets connectés et la confiance dans la sécurité des données transmises

L'essor des objets connectés pose la question de la sécurité de leur utilisation et nécessite la définition d'une normalisation de leur utilisation mais plus encore de garantir la protection des données personnelles ou du consentement. Le rapport précité du Conseil d'État relève ainsi que « *la sécurisation de l'internet des objets représente donc une urgence politique* ».

c. Les blockchains et l'enjeu primordial de la relation de confiance

La technologie des *blockchains* n'en pose pas moins des questions importantes.

La relation de confiance repose principalement sur le recours au cryptage mais elle n'est relative qu'au sein du réseau qui reste virtuel. Qu'est-ce qui permet de s'assurer que, dans le monde réel, la transaction a été assurée par la personne revêtue de la même identité ? Et le Conseil d'État d'en conclure qu'il convient de s'interroger sur la nécessité d'intervention des pouvoirs publics dans la certification des relations entre monde virtuel et monde réel.

2. Un cadre juridique ébranlé

Le développement des plateformes numériques se satisfait du minimum de régulation. C'est l'autorégulation non contraignante qui règne à travers le contrat, la relation de confiance ou encore le cryptage. Ce n'est pas sans effet sur la façon dont nos règles juridiques évoluent aujourd'hui. Le principe de loyauté, parfaitement connu du droit des contrats, irrigue désormais le droit appliqué au numérique.

Cette évolution s'accompagne par ailleurs d'une confrontation de deux visions divergentes quant à la protection des données personnelles. Dans son ouvrage précité, Olivier Iteanu oppose ainsi la *privacy* à la conception européenne de la vie privée.

La *privacy* a été précisée par la jurisprudence des cours américaines et pourrait se définir comme « *le fait que le citoyen a le droit qu'on le laisse en paix* ». En d'autres termes, elle vise essentiellement à protéger le citoyen de l'immixtion de l'État dans la vie et le domicile du citoyen. Elle s'inscrit par ailleurs dans une logique juridique différente comme le rappelle l'ouvrage d'Olivier Iteanu : « *le droit au respect de la vie privée a reçu la protection de la* common law*, non pas en tant que tel, mais plutôt en tant qu'extension du droit naturel du droit de la propriété* ». En somme, la *privacy* est rattachée à la propriété et emporte une conséquence importante : il est possible de la négocier et de la vendre d'autant qu'il n'existe aucunement de législation fédérale portant sur les données personnelles et partant, d'une instance de régulation.

A contrario, le droit européen, particulièrement français, rattache la vie privée à la personne. Elle ne constitue toutefois pas un droit absolu, des limitations pouvant y être apportée (sécurité nationale, sûreté publique, protection de la santé, …). Elle se traduit notamment par la protection particulière que le législateur a entendu apporter aux données personnelles en tant qu'elles sont susceptibles d'identifier directement ou indirectement une personne physique. La collecte et le traitement de ces données obéissent au régime juridique issu la loi informatique et libertés qui vise à empêcher toute manipulation de nature à attenter à la vie privée des citoyens.

Vie privée et données personnelles

« *Susceptibles de se recouper, informations relatives à la vie privée et données personnelles peuvent, sur certains points, être distinctes. Du fait de leur numérisation, toutes les informations sur la vie privée deviennent des données personnelles. Mais toutes les données personnelles ne concernent pas la vie privée. Les moyens juridiques de protection peuvent être distincts ou se compléter et se conforter. Il convient donc de les considérer dans leur diversité* ».

Source : DERIEUX Emmanuel - Nouveaux Cahiers du Conseil constitutionnel n° 48 (dossier : vie privée) - juin 2015 - pp. 21 à 33

Or, cette divergence de conception profite bien souvent au développement des plateformes numériques.

Elle a abouti à une collecte sans précédent de données personnelles en contradiction avec les dispositions juridiques. Une récente décision de la CNIL relève ainsi l'ampleur de la confrontation de visions s'agissant des données personnelles. Dans une décision du 26 janvier 2016 [(1)], la CNIL a mis en demeure Facebook de se conformer aux prescriptions de la loi du 6 janvier 1978 constatant l'étendue et l'importance des données collectées : informations fournies par les utilisateurs eux-mêmes (activité, contenus partagés et consultés), équipements utilisés, système d'exploitation des machines, navigateur, coordonnées GPS, numéro de téléphone mobile. Mais *Facebook* récupère aussi les données des sites tiers, y compris pour ceux qui n'ont donné aucun accord à cet effet. Facebook collecte aussi les données des entités de son groupe *via Instagram* ou *Whatsapp*. Elle a mis en demeure aux fins de « *collecter loyalement les données de navigation des internautes ne disposant pas de comptes FACEBOOK* » et afin que les utilisateurs « *puissent s'opposer à la combinaison de l'ensemble de leurs données à des fins publicitaires* ».

Elle se traduit aussi par l'imposition de clauses au sein des conditions générales d'utilisation (CGU) en contradiction flagrante avec le droit en vigueur. Bien souvent, en dépit de décisions de justice, ce n'est pas le droit français qui est applicable en cas de litige mais le droit des juridictions étrangères,

(1) Décision n° 2016-007 du 26 janvier 2016 mettant en demeure les sociétés Facebook Inc. et Facebook Ireland

particulièrement californiennes. Cette simple mention suffit à décourager toute personne désireuse d'exercer ses droits et quand bien même elle engagerait une action en justice, un temps certain s'écoulerait jusqu'à la résolution d'un conflit comme le rappelle Olivier Iteanu.

Ce quotidien est aujourd'hui le nôtre et le Conseil d'État résume parfaitement l'enjeu auquel nous sommes aujourd'hui confrontés : « *la création de nouvelles féodalités portées par des objectifs économiques et capitalistiques qu'il appartient à la puissance publique de réguler.* »

C. L'INTERVENTION DE LA PUISSANCE PUBLIQUE RESTE ENCORE PLEINEMENT JUSTIFIÉE

Popularisé par Lessig, le leitmotiv « *Code is law* » a été souvent interprété comme une injonction, celle visant à ne pas réglementer le développement du numérique. En réalité, cette formule constitue un puissant appel en faveur de la réglementation : la loi plutôt que le code. La loi présente l'avantage de la clarté alors que le code se caractérise plutôt par son ésotérisme et ses biais. Elle permet également de rétablir un certain équilibre entre les parties en neutralisant les éventuelles asymétries et présente l'avantage de la permanence quand le code évolue sans cesse.

1. Le droit national prévoit déjà des règles de protection

Avec le développement du numérique, des algorithmes et de l'intelligence artificielle, nombre de voix s'élèvent pour que le législateur définisse un cadre juridique adapté. En réalité, ce cadre existe aujourd'hui mais il reste particulièrement méconnu tant par des citoyens que des acteurs économiques. Ce constat a notamment été formulé en audition par les représentants d'ADEL, un organisme chargé de promouvoir une démarche éthique dans l'utilisation des algorithmes. L'encadrement existe déjà depuis 1978 comme l'illustre la synthèse du débat public confiée à la CNIL par la loi sur la République numérique [(1)].

La loi précise les conditions d'utilisation des « *données personnelles nécessaires au fonctionnement des algorithmes* » au travers des principes de finalité, de proportionnalité, de sécurité et de limitation de durées de conservation des données :

– l'article 10 de la loi 1978 prohibe la prise de décision par une machine sans intervention humaine lorsque celle-ci emporte des conséquences importantes. La synthèse de la CNIL précitée mentionne ainsi les décisions judiciaires ou l'octroi d'un crédit. Cela étant, l'usage est autorisé pour les autres décisions

(1) CNIL, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle *», synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique, décembre 2017.*

produisant des effets juridiques mais, dans ces cas, la loi prévoit que la décision « *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* » ;

– l'article 39 de la loi prévoit le droit pour les personnes d'obtenir, auprès de celui qui en est responsable, des informations sur la logique de fonctionnement de l'algorithme. Cet article permet de rétablir l'asymétrie d'informations.

En matière de santé, la pratique médicale constitue un exercice illégal lorsque la personne n'est pas titulaire d'un diplôme comme le prévoit l'article L. 4111-1 du code de la santé publique. Selon la CNIL, ce dernier pourrait trouver à s'appliquer aux dispositifs d'intelligence artificielle aussi bien qu'à la prise de décision par un algorithme seul. La synthèse du débat public rappelle que cette législation, datée du XIXe, avait été motivée pour lutter contre le « charlatanisme »… où l'on voit que les promesses de « lendemains qui chantent » en matière de santé ne constituent pas, loin s'en faut, des nouveautés !

Les citoyens, comme les entreprises, ont donc tout à redécouvrir du cadre législatif existant. Il importe qu'ils y soient sensibilisés. Parfaitement consciente de cet enjeu, la CNIL s'est depuis longtemps engagée et ce, bien avant ses homologues régulateurs européens, dans une logique d'accompagnement des acteurs en rappelant les dispositions existantes et en les déclinant à travers divers outils de référence.

2. Le droit européen : entre renforcement de la protection des données et aménagement de la régulation

Le projet de loi opère, quant à lui, plusieurs modifications de nature à renforcer la protection des données personnelles en cohérence avec la nouvelle réglementation européenne S'il opère un renversement de la logique de contrôle des protections de données, on retiendra surtout la promesse d'appliquer le droit à l'ensemble des acteurs du numérique, y compris ceux basés à l'étranger lorsque, bien évidemment, ils proposent une prestation de services aux résidents européens. Si l'on assortit cette disposition à l'approfondissement de l'arsenal répressif (possibilité de prononcer une amende dont le montant peut représenter jusqu'à 4 % du chiffre d'affaires), on mesure désormais l'importance de l'enjeu qui se présente pour les GAFA plus enclins à s'éviter les contraintes des lois européennes. Cet enjeu est primordial !

3. Un encadrement encore incomplet

Ces dispositions présentent toutefois des limites. Des angles morts subsistent, qui ne sont prévus ni par la loi informatique et libertés, ni par le droit européen.

S'agissant des données à caractère personnel, il importe de constituer un corpus éthique susceptible d'accompagner le recours aux algorithmes. Le label ADEL promeut l'éthique des algorithmes de traitement et des données numériques. Cette initiative montre la nécessité de promouvoir, sous le contrôle de la CNIL, une labellisation qui porterait sur la démarche de traitement de données à caractère personnel. L'objectif consisterait à « éprouver et tester le système algorithmique », dès sa conception (« *ethics by design* »). Les concepteurs du label ADEL, auditionnés par la rapporteure, plaident par ailleurs pour l'identification, notamment au sein de l'organe de gouvernance de l'entreprise, d'un « *directeur de l'éthique du numérique* » et qui pourrait être le « *garant du bon traitement éthique des données personnelles numériques* ». Le développement en parallèle de « *comités d'éthiques indépendants manipulant des données personnelles numériques* », au sein des entreprises et par branche professionnelle, devrait aussi permettre de renforcer cette démarche par la diffusion de bonnes pratiques.

La question des données à caractère non personnel constitue un second enjeu. Les algorithmes, appliqués à ces catégories de données, sont susceptibles d'entraîner des effets sociaux et économiques importants : les nouvelles méthodes d'apprentissage, ou comme l'évoque le rapport de la CNIL, l'optimisation des menus des cantines scolaires. Plus récemment, on rappellera l'enjeu relatif à la répartition des étudiants selon l'offre de formation existante. On pourrait aussi mentionner les questions posées par le recours aux algorithmes afin d'optimiser le taux d'occupation des lits d'un établissement de santé.

D'autres questions portent sur l'interdiction pure et simple du recours aux algorithmes dans des secteurs sensibles comme le domaine militaire ou encore dans le domaine génétique : le rapport de la CNIL se risque ainsi à évoquer une « *limitation du recours aux données (…) pour maintenir « le voile d'ignorance indispensable » à la pérennité de la mutualisation du risque* ».

La rapporteure ne prétend pas être exhaustive. Elle renvoie à cet effet aux lectures des rapports du Conseil d'État et de la CNIL sur ces enjeux primordiaux. Le législateur s'honorerait à découvrir ces réflexions, réinvestir (ou redécouvrir ?) notre culture juridique au regard des défis qui s'annoncent afin de proposer des évolutions en cohérence avec les principes qui fondent notre organisation sociale. Le projet de loi relatif à la bioéthique, annoncé pour le premier semestre 2019, sera sans nul doute l'occasion de fixer un certain nombre de repères juridiques.

II. LE NOUVEAU CADRE DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Le projet de loi relatif à la protection des données personnelles vise à prendre acte du cadre juridique défini par l'Union européenne en matière de protection des données personnelles, rassemblé dans un « *paquet* ».

1. Une protection portée par un cadre juridique européen et national

Aux termes de l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE), l'Union européenne (UE) est en effet compétente pour définir les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Sur ce fondement, l'UE a adopté deux décisions distinctes :

– un règlement européen (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel qui constitue le cadre général de la protection des données [(1)], plus couramment appelé RGPD ;

– une directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales [(2)].

a. La portée du règlement européen

L'article 288 du TFUE récapitule les différents actes adoptés par l'Union européenne qui constituent ce que l'on appelle le droit dérivé.

Le règlement revêt une portée générale et est « *obligatoire dans tous ses éléments* ». Il est par ailleurs directement applicable dans tout État membre, ce qui signifie qu'il n'est nul besoin de recourir à des mesures de transpositions législatives ou réglementaires. En théorie, le règlement constitue une norme précise qui se suffit à elle-même.

En l'espèce, l'article 99 du règlement dispose qu'il sera obligatoire dans tous ses éléments et directement applicable dans tout État membre à partir du 25 mai 2018.

Cela étant, si le règlement présente des mesures directement applicables, il prévoit plus d'une cinquantaine d'items pour lesquels les États membres sont amenés à en préciser le cadre ou à prévoir plus de garanties que n'en prévoit le droit européen. Ce règlement *sui generis* vise en effet à remplacer une directive

---

(1) 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) (Texte présentant de l'intérêt pour l'EEE).

(2) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

antérieure [1], qui avait dû faire l'objet de mesures de transposition nationales. Selon un rapport d'information de la commission des affaires européennes de notre assemblée [2], la Commission européenne a souhaité « *renforcer la cohérence de la protection des personnes, la sécurité juridique ainsi que la libre circulation des données à caractère personnel au sein du marché intérieur, en évitant les divergences de transposition* ». Néanmoins, certains États membres ayant souhaité maintenir une directive, le texte qui en est résulté semble être le résultat d'un compromis « *mêlant des dispositions harmonisées à de multiples renvois au droit national* ». L'annexe 1 du rapport précité présente ainsi l'ensemble des thèmes pouvant faire l'objet d'une mesure nationale. Y figurent notamment les dispositions relatives aux traitements de données sensibles, y compris de santé, génétiques ou biométriques, en application des considérants 51, 52, 53 du règlement ainsi que son article 9).

De manière plus générale, les États membres sont habilités à maintenir ou adopter des règles spécifiques pour certains types de traitement, particulièrement ceux entrant dans le champ de la saisine pour avis de la commission des affaires sociales. Il s'agit ainsi des traitements applicables aux données de santé, aux données génétiques ou du traitement du numéro d'identification au répertoire (NIR). Ces marges de manœuvre permettent ainsi de maintenir des dispositions déjà prévues par le droit en vigueur ou autorisent à adopter des mesures d'adaptation pour « *prendre en compte les évolutions technologiques et sociétales* », comme le souligne l'exposé des motifs du projet de loi.

b. Le champ d'application de la directive

La directive, quant à elle, lie tout État membre destinataire « *quant au résultat à atteindre* », tout en laissant aux instances nationales la compétence quant à la forme et aux moyens. En d'autres termes, il appartient à chaque État de prévoir dans son droit interne le cadre juridique permettant de parvenir au résultat défini par la directive : c'est tout l'enjeu de la transposition posée.

En l'espèce, la directive a pour principal objet d'encadrer le traitement des données personnelles par les « *autorités compétentes* à « *des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ». Son considérant 12 en précise le champ d'application. Il s'agit notamment de viser les activités menées par la police ou toute autre autorité répressive de nature à prévenir ou détecter

---

(1) 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) Mme Anne-Yvonne Le Dain et M. Philippe Gosselin, rapport d'information déposé en application de l'article 145 du règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française, Assemblée nationale, n° 4544, quatorzième législature, session ordinaire 2016-2017, 22 février 2017.

toute infraction pénale, y compris « *sans savoir au préalable si un incident constitue une infraction pénale ou non* ». Le même considérant étend le champ :

– à l'exercice de l'autorité par l'adoption de mesures coercitives, telles que les activités de police lors de manifestations, de grands événements sportifs et d'émeutes ;

– « *au maintien de l'ordre public lorsque cette mission est confiée à la police ou à d'autres autorités répressives lorsque cela est nécessaire à des fins de protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la société protégés par la loi, et de prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale* ».

2. L'articulation entre le droit de l'Union et le droit des États membres

La coexistence du paquet européen, applicable aux matières relevant de la compétence de l'Union, et des droits nationaux relevant des matières incombant aux États membres nécessite de se pencher sur leur articulation. Pour ce faire, il convient de se référer à l'article 9 de la directive précitée.

Cet article précise que si les traitements des données à caractère personnel relèvent des finalités prévues par la directive précédemment énoncées, il convient de se référer au cadre juridique de celle-ci. En revanche, lorsque ce traitement relève d'autres finalités, il convient de se référer au cadre général prévu par le règlement 2016/679, pour autant que l'activité relève de la compétence de l'Union européenne. Dans son avis portant sur le texte, le Conseil d'État a eu l'occasion de préciser le droit applicable aux traitements de données à caractère personnel présentant des finalités mixtes, soit qu'il relève des finalités prévues par la directive et le règlement, soit qu'il relève du champ de la directive ou du droit interne.

Le projet de loi n'opère pas cette articulation. Le Gouvernement a en effet fait le choix d'une rédaction permettant d'abord de satisfaire aux obligations européennes. Il n'en prévoit pas moins une habilitation par ordonnance aux fins de mise en cohérence des différents dispositifs. Cette ordonnance, qui serait publiée en septembre 2018, devrait aboutir à une réécriture globale de la loi informatique et libertés.

B. UNE RÉGULATION ASSOCIANT RESPONSABILITÉ DES ACTEURS ET CONTRÔLE *A POSTERIORI*

Fort du cadre juridique défini par le droit européen, le texte vise à mettre en conformité le droit national avec les nouvelles exigences prévues par celui-ci tout en précisant le régime du traitement des données sensibles et du NIR.

1. Les règles directement applicables

Plusieurs dispositions portées par le paquet européen sont directement applicables et ne nécessitent pas de transpositions particulières.

Le cadre juridique unifié, permis par l'édiction du règlement, permet de fixer des principes importants.

Élément essentiel, le règlement définit la notion de données à caractère personnel comme « *toute information se rapportant à une personne physique identifiée ou identifiable* ». Il définit aussi le champ matériel du traitement de données en précisant qu'il peut être tout ou partie automatisé ou non automatisé. Pour mémoire, la directive retient une approche identique.

Le règlement présente par ailleurs plusieurs particularités importantes qu'il importe de souligner.

● Son champ d'application, précisé par l'article 3, est étendu par comparaison au droit antérieur.

Le règlement s'applique ainsi dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à suivre leur comportement. En résumé, le droit européen s'applique chaque fois qu'un résident européen est directement visé en conformité avec la jurisprudence de la Cour de justice de l'Union européenne (CJUE). Dans son arrêt *Google* c/Espagne rendu le 13 mai 2014, la CJUE a, en effet, considéré que la directive était territorialement applicable [(1)]. La rapporteure se félicite de cette précision très importante apportée par le droit européen qui confirme la solution apportée par voie jurisprudentielle. Cette règle témoigne de la volonté concordante des États membres de faire valoir leur approche de la protection des données personnelles.

Le règlement étend par ailleurs aux sous-traitants (la personne physique ou morale ou l'autorité qui traite des données pour le compte du responsable du traitement) des obligations aujourd'hui imposées aux responsables de traitement de données (la personne ou l'autorité qui détermine des finalités et des moyens du traitement). L'approche du règlement, conforme à la position défendue par la France, vise à établir une responsabilité conjointe des responsables de traitement et des sous-traitants. Dans son considérant 81, le règlement stipule que le « *responsable du traitement ne devrait faire appel qu'à des sous-traitants présentant des garanties suffisantes* », celles-ci pouvant être présumées par l'approbation d'un code de conduite (article 40) ou l'application d'un mécanisme de certification (article 42).

(1) CJUE, Affaire C-131/12, 13 mai 2014.

Plusieurs objectifs sont par ailleurs assignés au règlement européen encadrant les données personnelles des personnes physiques faisant l'objet d'un traitement automatisé.

● Le règlement renforce le droit des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures.

Il réaffirme le principe du consentement, entendu comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». À cet effet, le responsable du traitement doit être en mesure de démontrer qu'un consentement a été donné. En cas de déclaration écrite, toute demande de consentement doit par ailleurs être formulée de façon distincte, compréhensible et aisément accessible. Le droit au retrait du consentement est par ailleurs prévu par le texte.

Parallèlement, le règlement prévoit de nouveaux droits pour les personnes dont les données font l'objet d'un traitement. Sans prétendre à l'exhaustivité, la rapporteure met en lumière les évolutions suivantes :

– l'article 8 prévoit des conditions particulières pour le traitement des données des mineurs de moins de 16 ans. En ce cas, le consentement est recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent toutefois décider d'abaisser l'âge, sans qu'il soit inférieur à 13 ans ;

– l'article 17 introduit le droit à l'effacement des données personnelles notamment lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées, pour retrait du consentement ou pour traitement illicite ;

– l'article 20 instaure un droit à la portabilité des données de nature à permettre à toute personne de maîtriser ses propres données. La disposition permet ainsi à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers.

● Le règlement s'inscrit par ailleurs dans une logique de responsabilité des acteurs du traitement des données. Alors que le fondement de la directive de 1995 reposait sur un régime équivalent à la police administrative (déclaration, autorisation), le règlement européen suppose une logique de conformité, impliquant la responsabilisation des acteurs ainsi que le contrôle et l'accompagnement du régulateur.

Les obligations pesant sur le responsable de traitement et le sous-traitant sont multiples.

Elles se caractérisent, à l'article 25, par des « *mesures techniques et organisationnelles appropriées* » afin de protéger les données « *dès la conception* » ainsi que « *par défaut* » : dans le premier cas, il s'agit de s'assurer dès la détermination des moyens du traitement et au long de celui-ci des mesures techniques afin de permettre la pseudonymisation ou la minimisation des données (« *privacy by design* ») ; dans le second cas, il convient de garantir que, par défaut, seules les données nécessaires au regard des finalités du traitement sont traitées (« *privacy by default* »).

L'article 30 impose, quant à lui, la tenue d'un registre des activités de traitement des données par son responsable en lieu et place des formalités administratives préalables.

À l'article 35, elles se déclinent par l'établissement d'une analyse de l'impact des opérations de traitement sur la protection des données à caractère personnel lorsque le recours à de nouvelles technologies est « *susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques* ». Cette analyse est obligatoire dans certains cas, particulièrement lorsque sont traitées à grande échelle les données sensibles visées à l'article 9 du règlement.

Elles se caractérisent, à l'article 37, également par la désignation d'un « *délégué à la protection des données* » par le responsable de traitement et le sous-traitant. Cette désignation est obligatoire lorsque le traitement implique une autorité publique ou un organisme public. Pour les organismes privés, cette obligation ne vaut que si 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 consistent en un traitement à grande échelle des données sensibles et des données à caractère personnel relatives à des condamnations pénales et à des infractions.

D'autres mesures sont également prévues telles que la notification d'une violation des données à caractère personnel ou encore la mise en place d'un code de bonne conduite ou de mesures de certification.

● Faisant suite à la suppression des formalités préalables, la régulation s'opère, dans le cadre d'un contrôle *a posteriori*, sous la responsabilité d'une autorité nationale de contrôle investie de pouvoirs d'enquêtes, de prescriptions administratives ou de sanctions et chargée de coopérer avec ses homologues des autres États membres dans le cadre d'opérations conjointes. Le règlement prévoit ainsi la possibilité d'émettre une amende administrative « *pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu* ».

2. Le projet de loi procède au toilettage du droit existant et tire profit de certaines marges de manœuvre permise par le règlement

Conformément au droit européen, le présent projet de loi s'inscrit dans les orientations définies par le règlement européen. Il modifie les dispositions contraires au règlement et met en conformité celles d'entre elles qui restent compatibles. Le projet de loi procède à la réécriture des dispositions pour lesquelles le règlement autorise des marges de manœuvres.

● Le droit comportera un champ extrêmement restreint des interdictions de collecte et de traitement des données. Celui-ci fait l'objet de l'article 8 qui traite des données sensibles, c'est-à-dire les données à caractère personnel « *qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux* » et qui méritent, à ce titre « *une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits* » [(1)].

Le projet de loi y mentionne explicitement les données génétiques ainsi que les données biométriques. Il opère des modifications d'ordre sémantique : l'origine raciale est assortie d'un adjectif qualificatif « *prétendue* » manifestant ainsi la nécessité de lutter contre toute discrimination de ce type sans adhérer aux théories établissant l'existence de races humaines distinctes. Les données sensibles comprendront aussi celles relatives à « *l'orientation sexuelle* » et non plus seulement à « *la vie sexuelle* ».

Ces données ne font pas l'objet d'un quelconque traitement sauf dans des cas spécifiques visant à respecter une obligation légale ou lorsqu'il est justifié pour l'exécution d'une mission d'intérêt public. La dérogation est aussi justifiée lorsque la personne concernée donne son consentement explicite ou lorsque le traitement vise à répondre à des besoins spécifiques, en particulier dans le cadre d'activités associatives ayant pour objet de permettre l'exercice des libertés fondamentales. Un certain nombre de dérogations sont déjà prévues par le droit en vigueur. Le texte en complète la liste, s'agissant particulièrement des traitements portant sur les données génétiques et biométriques mis en œuvre pour le compte de l'État.

Bien évidemment, comme c'est aujourd'hui le cas, les données de santé entrent dans la catégorie des données sensibles. Le projet de loi maintient cette interdiction et modifie l'économie de la loi informatique et libertés pour regrouper au sein d'un seul et même chapitre le régime juridique applicable aux données de santé. Aujourd'hui, pour connaître le droit applicable aux traitements relatifs aux données de santé, il faut combiner la lecture des articles 25, 27 et ceux compris dans le chapitre IX.

---

(1) Considérant 51 du règlement général sur la protection des données.

Le projet de loi maintient un régime d'autorisation préalable pour les traitements portant sur ces données tout en prévoyant, particulièrement s'agissant des données de santé, des procédures allégées.

● S'agissant des traitements portant sur les autres données à caractère personnel, le texte « *opère un renversement complet des logiques antérieures* » selon les termes employés par le Conseil d'État, en modifiant la forme du contrôle – passage d'un contrôle *a priori* à un contrôle *a posteriori* – ainsi que sa nature – les acteurs sont invités à évaluer le risque d'atteinte aux libertés et droits fondamentaux.

S'ensuit ainsi un allégement des formalités préalables au profit de la mise en place de procédures destinées à évaluer la conformité aux normes portées par le règlement européen et la loi, *via* le délégué à la protection des données, et de saisir l'autorité de contrôle, soit la CNIL, en cas d'atteinte potentiellement grave aux droits et libertés fondamentaux.

Ce transfert des responsabilités ne sera pas sans conséquence sur les acteurs publics et privés. Comme le relève le Conseil d'État, il requiert que le législateur adopte un dispositif juridique clair et rigoureux, ce transfert représentant un coût économique. Il importe en conséquence d'assurer un « *environnement robuste à leur prise de décision* ». Auditionné par la rapporteure, l'Inserm souligne ainsi que « *l'exigence cumulative de l'accomplissement de formalités administratives et de la documentation de la conformité pose de façon aiguë la question du modèle économique de la mise en œuvre du texte et des moyens nécessaires à cette double exigence et, en définitive, celle de l'effectivité de la règle et de son applicabilité* ». L'Inserm souligne aussi la nécessité de construire « *un standard européen homogène et ambitieux* » et suggère qu'un cadre homogène soit défini pour les traitements mis en œuvre à des fins de recherche dans le domaine de la santé « *afin d'éviter la mise en concurrence des systèmes juridiques au détriment de la France et de ne pas compromettre la compétitivité de la recherche française* ».

La CNIL n'est pas en reste et voit sa fonction de régulation fondamentalement évoluer. Ses ressources ont longtemps été concentrées sur les formalités préalables (déclarations et autorisations), instruments typiques de la police administrative. Le régime de sanctions se caractérisait par son cadre modeste et relativement peu dissuasif : jusqu'à la loi pour la République numérique, la sanction pécuniaire s'élevait à 150 000 euros [(1)] aux termes de l'article 46 de la loi du 6 janvier 1978.

Son rôle devra nécessairement muter dans ce nouvel environnement vers davantage d'accompagnement. Sur ce point, la rapporteure se félicite que les orientations du règlement européen aient déjà été anticipées par la CNIL. Force est de constater que l'autorité de contrôle a su élaborer une véritable doctrine

(1) Elle peut s'élever jusqu'à 3 millions aujourd'hui.

d'emploi à l'usage des responsables de traitement. Il suffit, pour s'en faire une idée, de se reporter au site internet de la CNIL qui met à disposition un certain nombre de fiches et guides pratiques ou encore d'informations réglementaires actualisées... Reçu en audition, le secrétaire général de la CNIL a confirmé ce basculement opéré il y a maintenant quelques mois. Le texte confère des responsabilités nouvelles à la CNIL, au-delà de l'établissement de recommandations, de lignes directives ou de méthodologies de référence. À l'avenir, elle pourra aussi agréer des organismes certificateurs et certifier des personnes, des produits, des systèmes ou des procédures.

Cette nouvelle régulation se traduit parallèlement par le renforcement des pouvoirs d'investigation (cadre d'intervention des agents, identité d'emprunt pour opérer les contrôles en ligne) et de sanctions de la CNIL.

Enfin, dernière évolution significative : l'européanisation des procédures et des décisions. Pour l'ensemble des traitements transnationaux, les autorités de protection des données devront se coordonner pour s'assurer de la conformité du traitement. Une autorité « chef de file » assurera le guichet unique de traitement, tout en effectuant la coordination des décisions et des sanctions avec ses pairs. Le rapport d'activité de la CNIL considère que cette dimension « *change considérablement les conditions d'intervention de la CNIL en matière répressive* », davantage même que le relèvement du montant maximal des sanctions pécuniaires.

Il convient donc que la CNIL dispose des moyens à la hauteur du défi qui s'ouvre pour ne pas obérer ses capacités opératoires.

3. Le régime du traitement des données sensibles et des données relatives au NIR

Le domaine de la santé combine la nécessaire protection de la santé et l'intérêt de la recherche. Le projet de loi participe de cet équilibre en préservant les acquis de la loi de modernisation de notre système de santé.

a. Le cadre juridique du NIR ne fait pas obstacle aux recherches scientifiques

Le projet de loi maintient le principe de formalités préalables s'agissant des traitements mettant en œuvre le NIR. Comme le souligne l'étude d'impact, le NIR « *constitue un numéro particulièrement signifiant* » notamment *« en ce qu'il comporte 13 caractères permettant de déterminer le sexe, l'année et le mois de naissance* ». Numéro unique et pérenne, il est susceptible de faire l'objet d'interconnexion dans différents autres fichiers.

Le projet de loi prévoit cependant un allégement des formalités liées aux traitements impliquant le recours au NIR.

● De l'avis de la CNIL, Le régime actuel était « *devenu, au fil des ans, largement incompréhensible par les responsables de traitement concernés* ». Il combine diverses autorisations accordées par la CNIL ou relevant du domaine législatif et réglementaire et déclarations préalables sans préjudice de la faculté de se dispenser de déclarations lorsque le traitement ne porte pas atteinte à la vie privée et aux libertés.

Sont aujourd'hui soumis à l'autorisation préalable de la CNIL, au titre de l'article 25 de la loi de 1978, les traitements portant sur des données parmi lesquelles figure le NIR ou qui requièrent sa consultation, y compris, par dérogation à l'article 27, les traitements qui ont exclusivement des finalités de recherche scientifique ou historique et pour lesquels une opération cryptographique lui substitue un code statistique non signifiant.

En application de l'article 27 de la loi précitée, sont actuellement soumis à l'autorisation réglementaire les traitements mis en œuvre pour le compte de l'État, d'une personne morale de droit public ou d'une personne privée chargée d'une mission de service public portant sur des données parmi lesquelles figure le NIR.

On peut enfin souligner la possibilité offerte par l'article L. 1111-8-1 du code de la santé publique de recourir au NIR dans la sphère médico-sociale comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales. Le régime est précisé par un décret en Conseil d'État, pris après avis de la CNIL. Il précise les modalités d'utilisation de cet identifiant, notamment afin d'en empêcher l'utilisation à des fins autres que sanitaires et médico-sociales. Par dérogation, le NIR peut être traité à des fins de recherche dans le domaine de la santé dans les conditions prévues au chapitre IX de la loi n° 78-17 du 6 janvier 1978 (*cf. développements ci-après*).

Par dérogation et en application du I *bis* de l'article 22, les traitements comportant le NIR, ou qui requièrent sa consultation, lorsqu'ils ont exclusivement des finalités de statistique publique et ne comportent pas de données sensibles, sont soumis au seul régime de la déclaration préalable. Le NIR doit également faire l'objet d'une opération cryptographique lui substituant un code statistique non signifiant. La déclaration préalable s'applique également aux traitements mis en œuvre afin de répondre à une alerte sanitaire en cas de situation d'urgence.

● Le projet prévoit que seule la publication d'un décret-cadre en Conseil d'État, pris après avis motivé de la CNIL, pourra autoriser les « *catégories de responsables de traitement* » et leurs « *finalités* ». Selon les informations transmises à la rapporteure, le décret devrait établir la liste de tous les responsables de traitement concernés sur le fondement des décisions prises par la CNIL. Ce choix rédactionnel devrait permettre de lever les inquiétudes soulevées par la CNIL dans son avis s'agissant des possibles blocages affectant les dispositifs innovants, particulièrement dans le cadre de la télémédecine.

Sont toutefois dispensés de l'autorisation, les traitements à des fins exclusivement statistiques, particulièrement ceux ne portant pas sur les données sensibles. Cette dérogation vaut également pour les traitements dont la finalité est exclusivement liée à la recherche scientifique ou historique ou encore pour les traitements mettant à la disposition des usagers un ou plusieurs télé-services. En ce cas, le NIR fait l'objet d'une opération cryptographique lui substituant un code statistique non signifiant.

Le décret cadre a également vocation à inclure les traitements dont la finalité répond à une alerte sanitaire en cas d'urgence lorsqu'il est recouru au NIR.

Par dérogation, les données de santé utilisant le NIR sont soumises aux formalités prévues par le chapitre IX dans sa version issue du projet de loi et maintiennent donc le régime d'assouplissement engagé par la loi de modernisation de notre système de santé. Cette disposition est essentielle pour les traitements à finalité de recherche. Lors de son audition, l'INSERM a ainsi souligné la nécessité de ne pas dresser d'obstacle juridique à une plus grande utilisation des bases médico-administratives et aux appariements nécessaires à la recherche et aux évaluations de santé publique, « *particulièrement utiles dans le cadre des registres de morbidité* » et « *des cohortes et, en particulier des cohortes financées par le programme investissement d'avenir ou par le volet recherche des plans de santé publique* ».

Les régimes juridiques applicables lorsque le traitement concerne à la fois le NIR et les données de santé

L'article 22 de la loi informatique et libertés, dans sa rédaction issue du projet de loi, vise à unifier le régime juridique des traitements recourant au NIR par le biais d'un décret-cadre. Toutefois, se pose l'articulation de ce dispositif avec celui prévu par le chapitre IX de la même loi lorsque sont en jeu des données de santé. On peut distinguer trois régimes différents :

– lorsque le NIR est apparié aux données de santé, le régime juridique relève du chapitre IX, l'objectif étant d'éviter une redondance des formalités (dernier alinéa de l'article 22 dans sa rédaction issue du projet de loi déposé) ;

– lorsque le NIR est utilisé dans le cadre dérogatoire de l'article 53, le traitement des données n'est pas soumis au chapitre IX mais relève du décret-cadre prévu par l'article 22. Sur ce point, il a été indiqué à la rapporteure que le décret-cadre listerait les acteurs concernés au vu des autorisations déjà accordées par la CNIL ;

– lorsque le NIR est utilisé en tant qu'identifiant national de santé (INS) des patients pour leur prise en charge à des fins sanitaires et médico-sociales, la lecture de l'article L. 1111-8-1 du code de la santé publique permet de conclure à l'application du droit commun des protections de données (absence de formalités préalables et évaluation du risque par le responsable de traitement).

b. Le cadre juridique des données sensibles maintient le principe d'interdiction assorti de dérogations

Le premier alinéa de l'article 8 pose le principe de l'interdiction du traitement portant sur des données sensibles qui ont trait à l'intimité de la personne ou sont susceptibles de donner lieu à des discriminations. Le projet de loi étend le champ des données sensibles aux données génétiques et conforte le régime de protection tenant aux données de santé.

i. Les données génétiques constituent une nouvelle catégorie de données sensibles

L'énumération actuelle des données sensibles ne correspond pas à la lettre du règlement. Le projet de loi modifie à cet effet la portée de l'article 8 pour étendre aux données génétiques le principe d'interdiction, les élevant au rang de données sensibles.

Le droit actuel est cependant déjà protecteur des données génétiques s'agissant des traitements automatisés. Ces derniers sont soumis à l'autorisation de la CNIL, 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. Ces dispositions restent inchangées.

Par dérogation, le II de l'article 8 prévoit les cas dans lesquels les données peuvent être traitées (consentement exprès, données rendues publiques, etc..). La dérogation prévue pour les traitements mise en œuvre par l'État portant sur les données génétiques dans l'exercice de ses prérogatives de puissance publique ou aux fins d'authentification ou d'identification est également maintenue et n'est pas modifiée aux termes du projet de loi.

ii. Le régime juridique des données de santé maintient globalement le niveau de protection existant

L'innovation, l'irruption des nouvelles technologies de l'information et la communication, la perspective du *big data* ainsi que l'adoption récente du règlement européen ont pu entretenir l'idée qu'aucun texte n'encadrait les données de santé, leur collecte ou leur traitement. Cette perception est évidemment erronée et traduit l'idée, qu'au-delà des textes, une acculturation est encore nécessaire. Nous traitons des données de santé sans le savoir comme M. Jourdain faisait de la prose sans le savoir. Dans un contexte de responsabilisation des acteurs, il importe d'avoir une approche précise des enjeux.

Selon une enquête de l'IFOP réalisée en 2013, seuls 14 % des 300 chefs d'entreprise interrogés estimaient connaître « *très bien* » la législation en vigueur. *A contrario*, près de deux sur cinq reconnaissent qu'ils la connaissent mal, voire très mal. Or la méconnaissance de la réglementation est susceptible d'engager la responsabilité de ces acteurs.

Le régime juridique des données de santé et de leur traitement combine les dispositions de la loi de 1978 précitée et les récentes évolutions apportées par la loi de modernisation de notre système de santé. Si le règlement européen n'abaisse pas le niveau de protection, déjà élevé en France, des ajustements sont néanmoins opérés par le projet de loi.

4. Le cadre juridique applicable aux données de santé

a. La notion de données de santé : un enjeu fondamental

En l'absence de définition légale, le champ des données de santé résultait auparavant des décisions jurisprudentielles, françaises comme européennes. L'article 4 du RGPD met fin à cette absence de base légale. Le périmètre couvre les « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

Cette définition reprend la formulation du comité d'experts sur la protection des données du Conseil de l'Europe. Dans un rapport explicatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, il est ainsi indiqué que les données de santé couvrent « *les informations concernant la santé passée, actuelle et future, physique ou mentale d'un individu. Il peut s'agir d'informations sur un individu bien portant, malade ou décédé* » [(1)].

Du reste, le considérant 35 du règlement reprend cette approche intemporelle. Les données se rapportent à l'état de santé passé, présent ou futur. Il donne plusieurs exemples de nature à mieux cerner l'approche retenue. Il en résulte que la définition européenne embrasse la dimension médicale des données de santé en établissant un lien entre le recueil des données et leur contexte d'utilisation : informations en vue de bénéficier d'un service de soins de santé ou collectées en vue de bénéficier de la prestation de ce service (numéro, symbole ou élément spécifique d'identification unique attribué à une personne physique), informations obtenues lors de test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques, …

Cela étant, il existe encore des données à caractère personnel se situant dans une zone indéterminée et qui peuvent révéler des informations sur l'état de santé d'un individu. Avec le développement des objets connectés et du *Quantified self*, des informations peuvent être collectées et traitées hors d'un contexte médical. Les données brutes qui sont transmises ne renseignent pas directement sur l'état de santé d'une personne mais il est toujours possible d'en déduire des indications relatives à sa santé.

---

(1) Conseil de l'Europe, Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, n° 108, 28 janvier 1981.

En réponse à une demande de la Commission européenne, Le G 29 (1) a précisé le périmètre des données de santé. Les données brutes, d'apparence inoffensive ou neutre, sont considérées comme des données de santé si elles permettent, en elles-mêmes ou combinées avec d'autres, de tirer des conclusions sur l'état de santé ou les risques de santé d'une personne. Le G 29 considère qu'entrent également dans le champ des données de santé, les conclusions elles-mêmes qu'elles soient fidèles, légitimes ou adéquates.

Ces développements montrent à quel point il importe que tous les acteurs aient conscience des finalités pour lesquelles les données de santé peuvent être amenées à être collectées et traitées. Légitimement soucieux de préserver leur vie privée, nos concitoyens restent plus que jamais acteurs de leur propre protection. On soulignera que le consentement exprès comme la divulgation des données personnelles suffisent à mettre en œuvre des traitements sur simple déclaration. Il est donc primordial de maintenir un degré élevé de sensibilisation de nos concitoyens à cet enjeu. Cette sensibilisation n'en est pas moins aussi importante pour les responsables de traitement des données et leurs sous-traitants. Il leur importe de s'interroger sur les finalités qu'ils entendent poursuivre avec leurs traitements. Dans un environnement permettant le croisement des données, considérablement multipliées par l'élaboration d'algorithmes, toute mise en place d'un traitement, particulièrement sur les données de santé, suppose de s'interroger sur le régime de protection adapté. C'est vrai pour les traitements pour lesquels les données collectées répondent explicitement aux finalités prévues par le législateur. Cela l'est tout autant, et avec un degré d'exigence élevée, pour les données se situant dans la « *zone grise* ». Cet enjeu suppose que le régulateur soit en mesure de définir une doctrine en lieu avec les acteurs concernés. Il implique également, qu'en contrepartie de la responsabilisation des acteurs, aucun obstacle ne soit opposé au contrôle exercé par le régulateur et aux éventuelles sanctions qu'il pourra prononcer.

b. Le régime juridique des données de santé

Ce cadre étant posé, il importe ensuite d'identifier le régime juridique applicable aux données de santé.

Le régime juridique de protection des données de santé s'inscrit dans le cadre du secret médical et de la loi du 6 janvier 1978 s'agissant de leur collecte et de leur traitement.

i. La protection offerte par le respect du secret médical

Lorsqu'il est question de la protection des données de santé, particulièrement dans le cadre de l'utilisation des technologies de l'information et de la communication, le rapprochement avec le cadre protecteur de la loi « informatique et libertés » est opéré immédiatement. Il n'en reste pas moins vrai

(1) Groupement des Autorités de protection des données personnelles européennes.

que la plus ancienne des protections des données de santé réside dans le secret médical.

L'article L. 1110-4 du code de la santé publique dispose ainsi que tout patient a droit au respect de sa vie privée et au secret des informations la concernant. Le même article dispose que « *ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes* ». De ce fait, tous les professionnels, les établissements de santé ainsi que les hébergeurs de données de santé et leurs sous-traitants sont soumis au secret médical et doivent en assurer le respect.

Cela étant, la loi de modernisation de notre système de santé a sensiblement modifié la portée du secret médical afin de permettre la meilleure prise en charge possible du patient. Le texte instaure ainsi le dossier médical partagé impliquant le stockage des données auprès d'un hébergeur spécifiquement titulaire d'un agrément délivré par le ministère de la santé. Il prévoit par ailleurs la possibilité de partager les informations concernant le patient, consacrée dans le cadre de la notion de l'équipe de soins au sens de l'article L. 1110-12 du code de la santé publique.

ii. La protection offerte par la loi « *informatique et libertés* »

La collecte et le traitement des données de santé s'inscrivent, pour leur part, dans le cadre prévu par la loi du 6 janvier 1978. Le caractère sensible de ces données a amené le législateur à adopter des dispositions spécifiques.

● Une interdiction de principe assortie d'exceptions

Ce régime est par principe celui de l'interdiction telle que formulée au I de l'article 8 de la loi du 6 janvier 1978 relatif aux données sensibles : « *il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître directement ou indirectement (…) qui sont relatives à la santé (…)* ». Par dérogation, cette interdiction ne s'applique pas dans des cas limitativement énumérés.

Selon les finalités, la mise œuvre suppose une déclaration auprès de la CNIL (article 22), une autorisation par celle-ci (article 25, IV de l'article 27 et chapitre IX) ou encore une autorisation par la voie réglementaire après avis de la commission (articles 26 et 27). D'une façon générale, la délivrance d'autorisation intervient dans des délais jugés trop longs et « *incompatibles avec les exigences du monde économique actuel et la performance publique* » ainsi que le souligne l'étude d'impact annexée au projet de loi. Par ailleurs, l'existence de nombreuses dispositions rend inopérante la protection de la vie privée des citoyens, lesquels sont tenus insuffisamment informés de l'utilisation de leurs données personnelles.

On retiendra notamment que l'interdiction ne s'applique pas en cas de consentement exprès de la personne concernée sauf si la loi l'exclut ou lorsque les données en question sont rendues publiques par la personne concernée. Les traitements nécessaires « *aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé* » [(1)] et mis en œuvre par un professionnel de santé ou toute autre personne soumise au secret professionnel ne sont pas non plus soumis à l'interdiction.

● Les principales dérogations

L'article 8 formule aussi d'autres dérogations. Par principe, les traitements automatisés de données de santé font l'objet d'un régime d'autorisation accordé par la CNIL sauf disposition spéciale. Un régime spécifique est prévu pour les traitements de données à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

Le régime des données de santé couvre ainsi plusieurs cas de figure.

Pour les données faisant l'objet d'une procédure d'anonymisation, l'article 8 de la loi précitée dispose qu'une autorisation de la CNIL est requise dans les conditions prévues par l'article 25 de la loi.

Les données justifiées par un intérêt public représentent le deuxième cadre dérogatoire. Le I de l'article 25 de la loi du 6 janvier 1978 prévoit ainsi le cas des données parmi lesquelles figure le NIR ou requérant sa consultation. Une autorisation est ainsi accordée par la CNIL dans un délai de deux mois, renouvelable une fois, l'absence d'autorisation étant réputée rejetée. Ce régime d'autorisation vaut aussi pour les traitements destinés à des finalités de recherche scientifique ou historique à condition que le NIR ait fait l'objet d'une opération cryptographique « *lui substituant un code spécifique non signifiant* ». Dans le cas particulier des traitements mis en œuvre pour le compte de l'État, par les personnes morales de droit public ou de droit privé gérant un service public, l'autorisation prend, selon le cas, la forme d'un décret en Conseil d'État ou d'un arrêté, après avis motivé de la CNIL (article 27).

Par exception, le régime de la déclaration préalable est requis pour les traitements de données de santé mis en œuvre par les entités chargées d'une mission de service public relatives aux situations d'urgence ou d'alerte sanitaire (article 22).

Les traitements « *nécessaires à la recherche, aux études et évaluations dans le domaine de la santé* » relevant du chapitre IX constituent le troisième cadre dérogatoire.

---

(1) Cette dérogation a permis la mise en place du dossier médical partagé.

Les traitements « *nécessaires à la recherche, aux études et évaluations dans le domaine de la santé* » sont autorisés dans le cadre prévu par le chapitre IX de la loi précitée, soit des articles 53 à 61. Ce chapitre couvre les traitements « *ayant une finalité d'intérêt public* ».

L'article 193 de la loi de modernisation de notre système de santé a procédé à la révision des conditions d'accès aux bases médico-administratives qui s'articulent évidemment avec la loi informatique et libertés.

Cette évolution est indispensable au développement des nouvelles méthodes de recherche fondées sur l'exploration et l'analyse des données de santé. C'est pourquoi le législateur a décidé du regroupement de bases de données [(1)] au sein du système national des données de santé (SNDS), placé sous la responsabilité de la caisse nationale d'assurance maladie. Six finalités sont assignées au SNDS parmi lesquelles l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ou encore la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.

Le principe retenu est double : ouverture large des bases de données et respect de la confidentialité des données et de la vie privée des personnes.

Ont vocation à être ouverts à tous, les jeux de données extraits de ces bases (les jeux de données agrégées ou d'échantillons dans le cadre d'une homologation par la CNIL) dans la mesure où l'anonymisation est garantie.

Pour les données présentant un risque de ré-identification, le principe d'accès est commandé par l'intérêt public, deux modalités d'accès ayant été définies :

– l'accès direct et permanent pour certaines institutions et organismes chargés d'une mission de service public [(2)] ;

– une autorisation de la CNIL est nécessaire pour les projets spécifiques présentés par les autres utilisateurs à deux exceptions près. Elle n'est pas requise pour les « *catégories les plus usuelles de traitement* » : une procédure d'examen simplifié est prévue *via* le respect de méthodes de référence. La loi a par ailleurs encadré les conditions d'accès en formulant deux finalités interdites à savoir, la promotion commerciale des produits de santé et la modulation des contrats d'assurance.

Deux circuits de prises de décisions sont ensuite prévus.

---

(1) Notamment, les données issues du programme de médicalisation des systèmes d'information (PMSI), du système national d'information interrégimes de l'assurance maladie (SNIIRAM) et des données sur les causes de décès mentionné à l'article L. 2223-42 du code général des collectivités territoriales.

(2) Décret n°2016-871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

– s'agissant des recherches impliquant la personne humaine, l'autorisation de la CNIL intervient après l'avis d'un comité de protection des personnes (CPP) y compris lorsqu'elles impliquent un appariement avec les données du SNDS.

– s'agissant des études, évaluation ou les recherches n'impliquant pas la personne humaine, l'Institut national des dépenses de santé (INDS) constitue le guichet unique des demandes d'accès au SNDS qu'il transmet au comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES). L'autorisation de la CNIL intervient après l'avis du CEREES.

Toutefois, six types de traitements ne ressortissent pas à ce cadre, par exemple ceux qui concernant le suivi thérapeutique ou médical des patients ou encore ceux relatifs aux remboursements ou aux contrôles effectués par l'assurance maladie obligatoire. Ces derniers relèvent selon les cas de la déclaration ou de l'autorisation préalable.

Le dispositif, fonctionnel depuis le mois d'août 2017, est positivement jugé par l'INDS. Au 10 janvier 2018, le nombre de dossiers soumis s'élève à 162, issus majoritairement d'organes publics. Deux tiers de ces dossiers entraient dans le cadre de la procédure faisant intervenir le CEREES, le dernier tiers ne relevant pas de la compétence de l'INDS ou pouvant faire l'objet de la procédure simplifiée. Le CEREES s'est réuni quatre fois et a pu examiner « *en moyenne 23 dossiers par session qui ont abouti à 63 % d'avis favorable ou avis favorable avec recommandations ». 4 % des dossiers ont reçu un avis défavorable. La CNIL a autorisé 40 % des dossiers qui lui ont été soumis dans un délai moyen de 3 mois après la soumission du dossier à l'INDS* ».

● Les principes clé guidant le traitement et la collecte des données de santé à caractère personnel

Plusieurs principes commandent la collecte et le traitement des données de santé à caractère personnel.

Le principe de finalité traduit l'idée que les informations ne peuvent être recueillies et traitées que pour un usage déterminé et légitime.

Le respect du droit des personnes commande également que, lors de la collecte des informations qui les concernent, les personnes doivent être clairement informées des objectifs poursuivis, du caractère obligatoire ou facultatif de leurs réponses, des destinataires et des modalités d'exercice de leurs droits au titre de la loi informatique et libertés (droit d'accès, de rectification et d'opposition).

Cette protection se traduit par le principe du consentement, consacré à l'article 7 de la loi, cette prescription n'étant toutefois pas obligatoire si le traitement satisfait à l'une des cinq obligations formulées par le même article. Par ailleurs, l'obligation d'information ne s'applique pas dans certaines situations. Le droit commun applicable des données à caractère personnel prévoit une dérogation pour les traitements constitués pour conserver des données à des fins historiques,

statistiques ou scientifiques. L'obligation d'information ne s'impose pas non plus lorsque la personne a déjà été informée, que l'information se révèle impossible ou exige des efforts disproportionnés.

L'obligation d'information s'applique également dans le cadre particulier des traitements de données de santé à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé. Ce sont les dispositions de l'article 57 de la loi du 6 janvier 1978 qui s'appliquent à l'exception des travaux portant sur des données non directement identifiants et concernant des services de l'État ou de la sécurité sociale, l'obligation d'information est assurée dans des conditions définies par décret en Conseil d'État.

Deux dérogations sont cependant prévues en faveur des traitements ayant pour finalité la recherche médicale si, pour « *des raisons légitimes* », le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave ou que les données ont été initialement recueillies pour un autre objet que le traitement et que les personnes concernées ne peuvent pas être retrouvées. En ce dernier cas, une dérogation est alors demandée à la CNIL dans le cadre de la procédure d'autorisation.

Enfin, le législateur a aussi tenu à consacrer le droit à l'oubli, à travers la conservation des données pour une durée strictement limitée et adaptée aux besoins du traitement.

c. Le nouveau régime prévu combine protection élevée des données de santé et responsabilisation des acteurs

Le projet de loi regroupe au sein du chapitre IX l'ensemble des dispositions relatives aux données de santé. Par souci de simplification, ce chapitre couvre l'ensemble des traitements relatifs aux données de santé qu'elles impliquent ou non le NIR, à l'exception notable des traitements de données de santé mis en œuvre par les entités chargées d'une mission de service public relatives aux situations d'urgence en cas d'alerte sanitaire ; en ce cas, le traitement est soumis au droit commun de l'analyse d'impact ou, en cas d'utilisation du NIR, au régime prévu par le décret-cadre. Ainsi que le souligne le Conseil d'État dans son avis annexé au dépôt du projet de loi, « *le Gouvernement a choisi d'employer les facultés qui lui sont reconnues pour le traitement des données de santé* ».

L'article 13 comporte un dispositif général, au sein d'un chapitre IX dont l'économie a été revue, permettant de couvrir les traitements portant l'ensemble des données de santé présentant une finalité d'intérêt public (section I) et un dispositif spécifique couvrant le cas particulier des traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé (section II). En cela le texte ne modifie pas le régime de protection des données de santé qui constituent toujours des données sensibles au sens de l'article 8 de la loi du 6 janvier 1978. Il ne fait qu'identifier au sein d'un chapitre IX des dispositions relevant des articles 25 et 27 d'une part, du chapitre IX dans sa rédaction actuelle

d'autre part. Enfin, le régime juridique maintient un régime d'exonération pour certains traitements comme c'est aujourd'hui le cas outre les cas prévus par l'article 9.2 du Règlement.

Conformément à l'esprit du règlement, la nouvelle logique de responsabilisation (*Accountability*) conduit à supprimer la plupart des traitements préalables y compris pour les données de santé (*cf.* annexe I).

Cet objectif fait de la déclaration de conformité aux référentiels, aux méthodologies de référence et le respect des règlements types, le principe, et l'autorisation par la CNIL, l'exception. Dans ce dernier cas, le texte prévoit la saisine de l'INDS par la CNIL ou son auto-saisine pour évaluer l'intérêt public du traitement. En tout état de cause, le projet de loi maintient le délai de deux mois dans lequel la commission est amenée se prononcer. Surtout il en modifie la portée puisque l'absence de décision est réputée favorable. Cette évolution constitue une réelle avancée tant pour les acteurs économiques que pour l'INDS. Elle n'en constitue pas moins un réel défi pour la CNIL. La rapporteure estime néanmoins que ce renversement de perspective est important pour que notre pays conserve le *leadership* en matière d'exploitation de données de santé surtout dans un écosystème numérique qui nécessite une réactivité très importante et notamment face aux GAFA. La qualité du recueil des données autant que leur nombre constitue un réservoir important d'informations susceptible de mieux ajuster notre politique de santé publique. Cela étant, il importe que cette évolution s'accompagne d'un renforcement substantiel des effectifs de la CNIL car il ne s'agit pas d'opposer liberté et protection mais justement de trouver un équilibre entre ce qui permet de mener une stratégie de santé cohérente et prospective et le droit des citoyens à être assuré d'un haut niveau de protection de ses données.

Il préserve également la faculté, par décision unique, d'autoriser à un même demandeur la possibilité d'opérer des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques.

Le texte maintient par ailleurs les règles spécifiques relatives au droit des personnes mineures dans le cadre des traitements à des fins de recherche comme le prévoit à cet effet le Règlement de l'Union. En particulier, le mineur de 15 ans ou plus s'est vu reconnaître le droit de s'opposer à ce que les titulaires de l'autorité parentale aient accès aux données le concernant, recueillies au cours de la recherche, de l'étude ou de l'évaluation, et le droit de s'opposer à ce qu'ils soient informés de l'existence même du traitement de données en cause si le fait d'y participer conduit à révéler une information sur une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale en application des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique ou si les liens de famille sont rompus.

Ces dispositions avaient été consacrées par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Leur maintien est indispensable pour permettre l'élaboration de politiques de prévention ou de prise en charge adaptées, s'agissant particulièrement de la lutte contre les drogues et les conduites addictives. En effet, comme l'INSERM a eu l'occasion de le souligner lors de son audition, « *aucun adolescent ne dira quelle quantité d'alcool il consomme, s'il a des pratiques sexuelles à risque, combien de temps il consacre aux jeux électroniques s'il sait que ses parents peuvent être informés de ses réponses* ».

Enfin, il faut aussi préciser que n'entre pas dans le champ du projet de loi la modification des traitements de données relevant de l'article 26 relatif aux prérogatives de puissance publique ou aux fins d'authentification ou d'identification qui porte sur des données sensibles.

d. Une rédaction qui mérite quelques clarifications

Plusieurs difficultés d'applications ont été soulevées lors des auditions. Elles résultent tout d'abord de la définition par le règlement européen des données de santé. Elles concernent ensuite la possible confusion entre les règles applicables aux traitements à des fins de recherche, d'étude et d'évaluation et celles portant sur les autres traitements comportant des données de santé. Elles ont enfin trait à l'articulation entre le code de la santé publique et la loi du 6 janvier 1978 s'agissant de l'utilisation secondaire d'échantillons biologiques pour l'examen des caractéristiques génétiques à des fins de recherche scientifique.

● Reçus en audition par votre rapporteure, les organismes complémentaires d'assurance maladie (OCAM) ont fait part de leurs craintes relatives au régime juridique du traitement effectué à des fins de remboursement ou de contrôle. La clarification des données de santé, à travers la définition qui en est donnée par le règlement, tend désormais à considérer les données de remboursement, non plus comme des données administratives, mais des données de santé.

En l'absence de dérogation expresse, à l'instar des régimes obligatoires d'assurance maladie, les OCAM devraient appliquer le régime prévu par le chapitre IX soit l'autorisation de la CNIL à défaut de la déclaration de conformité alors qu'aujourd'hui le traitement des données administratives relève d'un régime plus souple. Selon la lecture qui est faite, seul le consentement exprès des adhérents permettrait de rester dans l'épure du cadre juridique, cette obligation étant susceptible de faire obstacle à l'exécution des contrats, notamment les contrats collectifs.

● Une deuxième difficulté soulevée concerne les traitements statistiques réalisés par l'Insee ou l'un des services statistiques ministériels comportant des données sensibles. Actuellement soumis au régime de l'autorisation préalable, les traitements statistiques sur les données sensibles n'y seraient plus soumis, y compris, selon l'INDS et l'INSERM, lorsque ces traitements portent sur des

données de santé par abrogation de l'article 25 et en l'absence de renvoi au chapitre IX.

Sur ce point, il a été indiqué à la rapporteure que la rédaction retenue à l'article 13 permettait de conclure, en creux, à l'application du régime juridique du chapitre IX. Ces traitements relèvent en effet du 7° du II l'article 8 de la loi informatique et libertés qui ne fait pas partie de la liste des traitements dérogatoires. La liste mentionne ainsi les 1° à 6 ° du II du même article 8.

● Des interrogations subsistent quant à l'articulation entre la loi du 6 janvier 1978 et le code de la santé publique s'agissant de l'utilisation secondaire d'échantillons biologiques pour l'examen des caractéristiques génétiques à des fins de recherche scientifique.

Le droit actuel, comme le droit proposé, prévoit le principe du consentement exprès des personnes concernées lorsque sont en jeu des traitements nécessitant le recueil de prélèvements biologiques identifiants. Cette disposition heurte de plein fouet la dérogation prévue par l'article L. 1131-1-1 du code de la santé publique qui a pour objet d'assouplir le régime de consentement des personnes à l'examen de leurs caractéristiques génétiques à partir d'éléments biologiques initialement prélevés pour une autre finalité. Cet article subordonne cette dérogation au respect de plusieurs garanties (finalité de recherche scientifique, information des personnes concernées et absence d'opposition, dérogation encadrée à l'obligation d'infirmation lorsque les personnes concernées ne peuvent pas être retrouvées). Mais faute de mise en cohérence, l'interprétation actuelle tend à faire du consentement exprès un élément opposable y compris aux recherches pouvant présenter un intérêt scientifique. L'INSERM souligne ainsi que les méthodologies de référence de la CNIL sont rédigées de telle sorte qu'elles conduisent à exclure l'utilisation secondaire d'échantillons biologiques de personnes décédées ou perdues de vue à des fins d'analyse génétique faute de pouvoir recueillir leur consentement.

Il a été indiqué à la rapporteure qu'une évolution sera prévue dans le cadre du prochain projet de loi relatif à la bioéthique.

Le projet de loi présente des évolutions bienvenues dans le domaine de la protection des données à caractère personnel. En opérant un basculement du contrôle *a priori* vers un contrôle *a posteriori*, le texte fait le pari que le respect du droit ne pourra être effectif qu'avec l'implication des entreprises et des administrations en charge des traitements de données. Il faut désormais être à la hauteur du rendez-vous. Le législateur y prend sa part en adoptant ce texte. Le pouvoir exécutif comme la CNIL feront œuvre de pédagogie pour faciliter l'accompagnement des responsables de traitements. Ces derniers devront porter une attention encore plus grande qu'aujourd'hui au droit de la protection des données personnelles. S'agissant enfin du citoyen, le consentement éclairé à l'utilisation de ses données supposera de sa part une attention de tous les instants.

TRAVAUX DE LA COMMISSION

La commission des affaires sociales procède à l'examen pour avis du projet de loi relatif la protection des données personnelles lors de sa réunion du mardi 23 janvier 2018.

Mme la présidente Brigitte Bourguignon. Mes chers collègues, notre ordre du jour appelle l'examen pour avis des articles 7, 9 et 13 du projet de loi relatif à la protection des données personnelles, examiné au fond à partir de ce soir par la commission des lois. Notre commission s'est saisie pour avis des articles portant notamment sur les données de santé. Sous l'influence du droit européen, la refonte du régime de protection de ces données ne pouvait évidemment pas nous laisser indifférents.

Mme Albane Gaillot, rapporteure pour avis. La protection des données personnelles n'est pas une préoccupation nouvelle pour le législateur. La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi « Informatique et libertés », était déjà la réponse du législateur aux craintes suscitées par l'interconnexion de fichiers à l'aide du numéro Insee.

Cette loi, fondatrice, nécessite aujourd'hui d'être actualisée au regard de l'enjeu sociétal que représente le numérique. Les nouvelles technologies informatiques ont modifié en profondeur nos usages. Elles concernent tous les aspects de notre vie quotidienne – loisirs, nouvelles formes de sociabilité, information, échanges ou développement économique. Elles génèrent également un nombre exponentiel de données.

Le règlement européen de protection des données (RGPD), comme le projet de loi dont nous sommes saisis pour avis, constituent une réponse appropriée à ces nouveaux enjeux. Le RGPD, qui entrera en vigueur le 25 mai 2018, vise à alléger les charges résultant des formalités préalables de déclaration ou d'autorisation de traitements des données personnelles.

Les modifications proposées par ce règlement visent aussi à responsabiliser davantage les acteurs : ils seront désormais tenus de se conformer au cadre de référence, élaboré en lien avec l'autorité de régulation, et de procéder à une analyse des risques d'atteinte aux droits fondamentaux et libertés. Par ailleurs, ces mêmes acteurs pourront faire l'objet d'un contrôle *a posteriori*. Le régime des sanctions est considérablement renforcé – jusqu'à 4 % du chiffre d'affaires s'agissant des amendes pécuniaires. Ces modifications devraient nous permettre d'améliorer nos capacités de contrôle, dans le cadre d'actions coordonnées au niveau européen entre les autorités régulatrices.

En outre, le principe de l'application du droit de l'Union européenne et de ses États est explicitement prévu, y compris pour les traitements opérés hors territoire de l'Union, s'ils concernent un résident européen.

Enfin, si le règlement présente des mesures directement applicables, il en prévoit plus d'une cinquantaine dont les États membres devront préciser le cadre ou pour lesquelles ils pourront notamment prévoir plus de garanties que le droit européen. C'est le cas des données sensibles, à l'instar des données de santé, qui entrent dans le champ de notre saisine.

Le projet s'inscrit dans ce mouvement et renverse la logique antérieure. Le principe de l'autorisation préalable, accordée par l'autorité de régulation – en l'espèce, la Commission nationale de l'informatique et des libertés (CNIL) – s'efface au profit d'une déclaration de conformité à un référentiel et d'un renforcement des capacités de contrôle. Cela étant, s'agissant des articles 7, 9 et 13 dont nous sommes saisis pour avis, les États membres ont la possibilité d'adapter leur réglementation, afin de prévoir un degré de protection des données à caractère personnel plus élevé et de garantir les droits fondamentaux et les libertés.

L'article 7 traite des données « sensibles » qui méritent, à ce titre, une protection spécifique, car le contexte dans lequel elles sont traitées pourrait entraîner des risques importants. Le projet prend ainsi acte de l'élévation des données biométriques et génétiques au rang de données sensibles, au même titre que les données de santé. Pour ces catégories, le principe reste l'interdiction de traitement, sauf dérogations strictement encadrées.

Le projet de loi précise également les droits attachés à la protection des citoyens faisant l'objet de traitements de données à caractère personnel. Surtout, il définit officiellement les données de santé, élevant ainsi le degré d'exigence applicable aux traitements de données qui ne relevaient jusqu'alors pas de ce périmètre. Ces données de santé couvriront désormais les « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

L'article 9 traite du numéro d'inscription au répertoire (NIR) des personnes physiques. Au fil des ans, le régime actuel était devenu incompréhensible pour les responsables de traitement. Il combinait diverses autorisations accordées par la CNIL ou relevant du domaine législatif et réglementaire, ainsi que des formules allégées. Le texte prévoit désormais qu'un décret en Conseil d'État listera les acteurs concernés. Il sera publié après avis motivé de la CNIL.

L'article 13 modifie le chapitre IX de la loi du 6 janvier 1978 afin qu'il regroupe l'ensemble des règles dévolues au traitement des données de santé. Les

dispositions sont actuellement dispersées – aux articles 25, 27 et au chapitre IX de la loi.

Par ailleurs, s'il allège les formalités dans l'esprit du RGPD, cet article n'opère pas de bouleversement dans les procédures. Le projet de loi conforte les évolutions apportées par la loi de modernisation de notre système de santé (LMSS), s'agissant de l'ouverture encadrée aux informations du système national des données de santé (SNDS). Il maintient aussi la possibilité d'apparier le NIR aux données de santé, sous le contrôle de la CNIL, tout en maintenant la possibilité d'effectuer des travaux de recherche de qualité.

Une évolution doit cependant être soulignée : désormais, en cas de demande d'autorisation, le silence gardé par la CNIL pendant plus de deux mois vaudra acceptation. Cette modification permettra d'accélérer le traitement des demandes tout en maintenant un haut niveau de recherche, donc d'innovation et de compétitivité.

Le texte présente enfin plusieurs défis. Le premier devra être relevé par les responsables de traitement. L'appropriation des normes et leurs impacts économiques ont été régulièrement abordés au cours des auditions. Une certaine anxiété demeure et peut se nourrir des confusions résultant des choix rédactionnels opérés par le Gouvernement. Sur ce point, ce dernier a indiqué que l'urgence commandait de toiletter le droit en vigueur afin de supprimer les règles en contradiction flagrante avec le droit européen. Mais l'article 20 du projet habilite également le Gouvernement à légiférer par ordonnance, afin de procéder à la réécriture de la loi du 6 janvier 1978.

Le second défi concerne la CNIL. Cette dernière a parfaitement anticipé les évolutions du RGPD. Elle a élaboré une doctrine d'emploi conforme aux nouvelles exigences, tout en opérant un basculement de ses services vers l'accompagnement des opérateurs publics et privés. Toutefois, les objectifs sous-tendus par la nouvelle logique de régulation nécessitent un renforcement de ses capacités opérationnelles, tant pour l'accompagnement que pour le contrôle. La puissance publique doit prendre ses responsabilités, afin de faciliter la transformation de la CNIL en un accompagnateur, et non plus simplement un contrôleur.

Le dernier défi concerne ceux que j'appelle les « acteurs de données », qu'ils soient citoyens producteurs de données ou responsables de traitement des données personnelles – professionnels de santé, acteurs industriels ou organismes de recherche. Le recueil du consentement, le droit à l'information, le droit de rectification, le droit à l'oubli, pour ne citer qu'eux, supposent une démarche éthique de la part des responsables de traitement, qui compte autant que la qualité des données recueillies, aussi bien lors de la collecte que lors du traitement et de l'analyse. Les données de santé requièrent une vigilance toute particulière. Aussi, me semble-t-il indispensable de saluer le développement des labels et certifications, prévu par le texte.

De leur côté, les citoyens, producteurs de données, doivent être particulièrement vigilants quant au consentement accordé à l'utilisation de leurs données personnelles, surtout de leurs données de santé, alors que notre univers tend à devenir complètement numérique. Un ambitieux chantier de sensibilisation doit être entrepris. L'hiatus important entre la légitime volonté de protéger ses données personnelles et une forme d'insouciance quand il s'agit de donner son accord dans le cadre de nos outils numériques quotidiens pose question. On voit ainsi des internautes publier des informations sur leur santé sur les réseaux sociaux…

Il nous faut donc à la fois adopter un cadre juridique sécurisant et développer une pédagogie adaptée à cet environnement en perpétuelle mutation. Telle est la voie tracée par ce projet et je vous invite à donner un avis favorable aux articles dont nous sommes saisis.

Mme Josiane Corneloup. Au moment où le numérique et la mobilité révolutionnent notre rapport au monde, il est bien évidemment impératif de mieux protéger les personnes contre les manipulations potentiellement malveillantes de leurs données. La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et la loi pour une République numérique du 7 octobre 2016 y répondent en partie. Toutefois, l'adoption du Paquet européen de protection des données à caractère personnel par le Parlement européen et le Conseil le 27 avril 2016 est l'occasion de renforcer notre droit face aux nouvelles menaces qui pèsent sur la vie privée. C'est ce que propose le présent projet qui adapte le nouveau RGPD à notre législation et transpose dans notre droit la directive européenne concernant les infractions pénales.

Vous l'avez évoqué, la philosophie d'ensemble du texte repose sur une logique de responsabilité renforcée des acteurs du traitement et de leurs sous-traitants. Les articles 7, 9 et 13 dont notre commission s'est saisie s'inscrivent pleinement dans ce nouveau paradigme juridique. L'article 7 élargit le champ d'interdiction de traitement des données sensibles aux données génétiques, biométriques et concernant l'orientation sexuelle d'une personne, tout en accordant des dérogations spécifiques à l'État, en cas d'utilité publique ou sécuritaire. Il s'agit d'une avancée importante en termes de protection de la part intime de l'être humain.

L'article 9 supprime le régime de déclaration préalable auprès de la CNIL, sauf pour les traitements réalisés par des personnes publiques ou privées qui mettent en œuvre le NIR ou par l'État en sa qualité de puissance publique. La responsabilisation des entreprises est donc à l'œuvre : la CNIL en assurera le suivi et le contrôle, il s'agit d'un dispositif équilibré et fluide.

L'article 13 s'applique aux traitements de données de santé, en établissant un recours à des référentiels et des méthodologies de référence homologués par la CNIL, tout en conservant la procédure de déclaration et d'autorisation

actuellement en vigueur, donc de formalité préalable pour le traitement à des fins de recherches scientifiques.

C'est sans doute dans le domaine de la santé que subsistent quelques écueils. Par exemple, le traitement du NIR des patients dans le cadre de la télémédecine est de nature à freiner le développement de dispositifs innovants – pourtant promus par le Gouvernement – puisqu'il nécessitera une autorisation par voie réglementaire. Nous comptons sur vos explications, madame la rapporteure, pour lever ce point d'interrogation marginal.

Malgré tout, ce projet marque une avancée pour la sécurité des données personnelles et le droit des personnes, qui pourront en outre demander l'effacement ou la récupération de leurs données. Aussi, le groupe Les Républicains le votera.

Mme Agnès Firmin Le Bodo. L'objet du projet de loi est de mettre le droit français en conformité avec le paquet européen relatif à la protection des données. Fruit d'un compromis dans lequel la France a pris toute sa part, cette directive a été adoptée par le Parlement européen et le Conseil le 27 avril 2016.

Il s'agit d'un domaine où la France a joué un rôle pionnier puisqu'elle a été l'un des premiers pays de l'Union européenne à se doter d'une législation globale de protection des données à caractère personnel avec la loi fondatrice du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et avec la création d'une autorité de contrôle chargée de veiller à son respect, la CNIL.

Dans la mesure où il s'agit d'un phénomène qui ne connaît pas de frontière, il était nécessaire d'agir au niveau européen. Les trois articles dont notre commission s'est saisie pour avis traitent des données sensibles, du numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et des données de santé.

Il convient de maintenir un cadre exigeant dans le traitement des données qui permette la recherche tout en ne pesant pas sur la compétitivité de notre pays. Ce projet de loi entend répondre à cette double exigence. Nous l'examinerons dans un esprit constructif et avec bienveillance car il va dans le bon sens.

Mme Nathalie Elimas. Sous ses aspects très techniques, ce projet renvoie à des enjeux politiques importants, qu'il s'agisse du sujet très sensible de la protection des données personnelles ou plus généralement du droit au respect de la vie privée. Ce sont autant de sujets d'inquiétude pour nos concitoyens et, à ce titre, je me réjouis que la commission des affaires sociales se soit saisie de ce texte pour avis.

Ce projet renforce la cohérence entre les pays de l'Union européenne : désormais, un organisme ne pourra plus choisir l'État dont le droit sera le plus avantageux pour lui. Il marque un progrès pour la protection des citoyens puisque la protection des données à caractère personnel est un droit fondamental inscrit

dans la Charte des droits fondamentaux de l'Union européenne. Pour cette raison, le groupe du Mouvement démocrate et apparentés le soutiendra.

Il constitue aussi un grand pas en avant pour la sécurité juridique des acteurs économiques mais aussi pour leurs capacités d'innovation. À titre d'illustration, le secteur de la santé, devenu stratégique en matière de données personnelles, bénéficiera d'un allégement des formalités préalables d'autorisation auprès de la CNIL.

Cette responsabilisation accrue des acteurs de santé ira de pair avec un renforcement en aval du contrôle. Elle favorisera notamment le déploiement de la télémédecine et de l'éducation thérapeutique.

Enfin, il est à noter que, dans sa rédaction actuelle, le projet de loi ne prévoit aucune disposition relative à l'âge de consentement pour le traitement de données personnelles. Il s'en remet au règlement européen qui l'a fixé à seize ans – l'autorisation des parents étant nécessaire avant – et qui a ouvert à chaque État membre la possibilité, dont se sont saisis l'Espagne et le Royaume-Uni, de l'abaisser jusqu'à treize ans. Ce point méritera sans doute débat.

M. Brahim Hammouche. Ce projet s'accompagne de nouvelles avancées sur la portabilité des données personnelles. La coopération européenne est renforcée, les autorités de protection des données personnelles devant adopter des décisions communes s'agissant du traitement des données transnationales, ce dont nous ne pouvons que nous réjouir.

Le groupe Mouvement démocrate et apparentés, et plus précisément mes collègues de la commission des lois, souhaite cependant sensibiliser les membres de notre commission à l'utilisation des données à caractère personnel collectées à partir d'outils numériques éducatifs. Les GAFA (pour Google, Apple, Facebook et Amazon) proposent des outils numériques gratuits pouvant concurrencer les espaces numériques sécurisés, qui sont privilégiés par le ministère de l'éducation. Nous pensons utile d'étendre à ces données les principes d'interdiction de traitement posés à l'article 7. Notre groupe déposera un amendement en ce sens en séance.

Mme la rapporteure. Madame Corneloup, vous redoutez que l'utilisation du NIR freine le développement de la télémédecine. Ce ne sera pas le cas. Un décret-cadre définira des catégories de responsables de traitement et autorisera des catégories de traitement. Les professionnels de santé ou les acteurs de traitement qui ont déjà obtenu une autorisation de la CNIL pourront continuer d'en bénéficier. Les responsables du Syndicat national de l'industrie des technologies médicales (SNITEM) que nous avons rencontrés se sont réjouis de la publication de ce décret-cadre. De portée plus générale, il ne nécessitera pas qu'un décret en Conseil d'État soit pris à chaque nouvelle demande d'autorisation.

Mesdames Elimas et Firmin Le Bodo, l'âge du consentement suscitera un débat à la commission des lois. Les adolescents entre treize et seize ans sont

souvent victimes de cyber-harcèlement. En qualité de rapporteure, je suis là pour poser un cadre : il est important d'instaurer une mesure plus protectrice, raison pour laquelle j'ai choisi de ne pas déposer d'amendement pour abaisser l'âge du consentement. Il y va aussi de la responsabilité des parents, auxquels il incombe de mieux former leurs enfants à l'utilisation des outils numériques.

Enfin, monsieur Hammouche, vous avez raison d'appeler notre attention sur les outils connectés. Un objet connecté produit-il des données de santé ? Non, il s'agit de données brutes mais nous savons que leur croisement aboutit à créer des données de santé qui, elles, relèvent du régime des autorisations. Nous étudierons votre amendement.

M. Adrien Quatennens. Contrairement aux apparences, ce projet ne vise pas une mise en cohérence entre le droit français et le droit européen, il libéralise la gestion des données personnelles et nous le déplorons. Il affaiblit le rôle de Commission nationale de l'informatique et des libertés, garante des droits des citoyens. En cela, il porte une atteinte grave au respect de la vie privée.

Des millions de nos concitoyens utilisent leurs smartphones et les réseaux sociaux et c'est leur vie privée qui est ainsi offerte aux multinationales spécialistes du *big data.*

Ce projet fait semblant d'ignorer la puissance des géants du *Net*. Il ne prend pas en compte le fait que des secteurs entiers ne reposent que sur l'exploitation des données personnelles et que, derrière l'apparente gratuite de nombreuses applications et sites internet, se cache la transformation du consommateur en produit. Le piratage des données de 57 millions d'utilisateurs de l'application Uber en novembre dernier est à cet égard alarmant.

Ce texte n'est clairement pas à la hauteur des enjeux.

Le profilage doit être interdit. Reposant sur un traitement automatisé, il vise à prédire des comportements grâce à l'analyse de données relatives au rendement au travail, à la situation économique, à la santé, aux préférences personnelles, aux intérêts, à la fiabilité, à la localisation, aux déplacements. Il permet, par exemple, à Facebook d'afficher sur votre fil d'actualité des publicités cohérentes avec le reste de vos activités, votre profession, vos besoins de vacances et même votre orientation sexuelle !

Nous devons aussi interdire le croisement de données non sensibles qui aboutit à créer des données sensibles. Imaginez ce que peut donner l'exploitation des données d'une application de *running* mesurant les performances sportives et de la géolocalisation, qui permet de savoir si vous consultez régulièrement un médecin traitant. Des données inoffensives en apparence regorgent de richesses pour les entreprises spécialisées dans leur collecte et leur gestion. Elles sont susceptibles d'être vendues au plus offrant et à ceux qui ont intérêt à connaître l'état de santé de leurs clients. Je pense aux assurances qui pourront en apprendre

beaucoup en passant outre le secret médical. Et ce n'est qu'un exemple des dérives que ce projet de loi ne prévoit pas de combattre.

Le Gouvernement sous-estime l'habileté de l'industrie du *web* à se procurer les données les plus rentables, au détriment du consentement et de la vie privée des personnes.

En fixant un cadre insuffisamment protecteur pour les individus et trop laxiste pour les entreprises, l'État se tirerait une balle dans le pied. Il accompagnerait l'extension infinie de la puissance des acteurs du *web* qui sont déjà, pour partie, aussi documentés que lui. Il ne se donnerait pas les armes nécessaires pour combattre les inévitables dérives d'un secteur dont chacun est de plus en plus dépendant. Bien sûr, ce n'est pas à l'État de régir le fonctionnement d'Internet mais il lui revient de garantir la protection des individus et le respect de la loi. Or nous en sommes visiblement encore bien trop loin.

Mme Caroline Janvier. Je salue la qualité du rapport, et l'accent qui y est mis sur l'esprit de ce paquet européen, qui prévoit un renforcement du rôle de la CNIL et une modification de sa mission, davantage dans un rôle d'accompagnement que de contrôle et de sanction, conformément à la volonté de ce Gouvernement pour ce qui concerne les rapports avec l'administration.

Il me semble par ailleurs qu'un véritable équilibre est trouvé entre le contrôle des données, notamment des données sensibles, et le respect de la liberté d'entreprendre et le développement du numérique.

Pour répondre à M. Quatennens, il ne faut pas renforcer la concurrence intra-européenne sur ces sujets, tout l'intérêt des directives européennes étant d'aller vers une harmonisation de la protection des droits sur ces questions très sensibles.

M. Sébastien Chenu. Contrairement à M. Quatennens, je ne crois pas que ce texte sous-estime la capacité des entreprises à utiliser les données personnelles, simplement le Gouvernement pratique le laisser-faire en toute conscience.

Ce texte a pour seul objet de se donner bonne conscience sans s'attaquer au fond du problème, nous ne le voterons pas en l'état.

Mme la rapporteure. Merci, madame Janvier, de votre soutien sans faille. Messieurs Quatennens et Chenu, il me semble que votre approche est similaire. Le cadre légal en France a près de 40 ans, il date de 1978. Il était fondé sur un régime d'autorisation, de déclaration préalable.

J'ai auditionné l'association des correspondants informatique et libertés, et je peux vous dire que la situation dans les TPE et PME était catastrophique. Ces entreprises n'appliquaient rien et faisaient du traitement de données sans rien déclarer, car elles ne connaissaient pas le droit.

Ce projet nous permet de braquer les projecteurs sur cette question, de restaurer la confiance des citoyens et des entreprises dans le numérique, de responsabiliser les entreprises, de donner un rôle important à la CNIL pour créer les référentiels, les règlements-types et les outils. De grandes entreprises ou des filières entières travaillent avec la CNIL, comme les assureurs, qui ont créé un pack de conformité sectoriel pour se mettre en conformité.

Aujourd'hui, les entreprises ou les acteurs de la recherche, du traitement ou de la collecte, manifestent un vrai souci de vigilance. Il n'y a aucune volonté de malveillance. Oui, des croisements de données se font parfois. Moi aussi, j'ai un smartphone qui compte mon nombre de pas, et j'ai signé quelque part pour donner mon accord. Oui, ce projet de loi répond à ce problème en prévoyant justement que ces données, parce qu'elles peuvent être croisées, deviennent des données de santé. Elles répondent ainsi à un régime spécifique d'autorisation et de mise en conformité.

Il y a donc un contrôle et une obligation pour l'entreprise de se mettre en conformité avec des référentiels ou des règlements-types. Et si ce n'est pas fait, la CNIL a des pouvoirs de sanction démultipliés, jusqu'à 4 % du chiffre d'affaires.

Le projet répond donc à l'ambition de protéger les citoyens et de responsabiliser. Il préserve la liberté de créer et de rechercher et prévoit des protections pour les citoyens. Le droit à la protection et le droit à l'oubli ne sont pas abordés par les articles qui font l'objet de la saisine de notre commission, mais ils créent de vraies protections. À nous, législateurs, d'être plus pédagogues à ce propos. C'est une matière compliquée, et plus nous serons pédagogues, plus le droit sera accessible et plus les citoyens seront protégés.

La commission en vient à l'examen pour avis des articles.

Suivant l'avis de la rapporteure, elle émet un avis ***favorable*** *à l'adoption des articles 7, 9 et 13,* ***sans modification.***

Puis elle émet un avis ***favorable*** *à l'adoption de l'ensemble du projet de loi,* ***sans modification.***

ANNEXE 1

L'ENCADREMENT DU TRAITEMENT DES DONNÉES DE SANTÉ AUX TERMES DU PROJET DE LOI DÉPOSÉ

Le caractère sensible des données de santé se traduit par une interdiction de principe de leurs traitements sauf dérogation. Le règlement laisse par ailleurs aux États membres une liberté d'appréciation susceptible de renforcer le niveau de protection de ces données. Par ailleurs, le régime s'accorde avec l'esprit de la réforme, consistant à responsabiliser les acteurs et à basculer des formalités préalables au profit d'un accompagnement et d'un contrôle renforcé.

Le traitement des données de santé obéira à trois régimes distincts.

1. Les traitements relatifs aux données ne relevant pas du chapitre IX

Certains traitements s'inscrivent dans le cadre de la déclaration préalable nécessitant la conformité aux exigences européennes fondées sur l'analyse critique opérée par les responsables de traitement d'une part, l'accompagnement et les contrôles opérés par l'autorité de régulation d'autre part. Ils relèvent des dérogations prévues par la section, particulièrement l'article 53 de la loi informatique et libertés de 1978 dans sa rédaction issue du projet de loi. Le régime est donc celui du droit commun du règlement (analyse des risques, responsabilité du traitement) sans préjudice des dispositions prévues par le code de la santé publique (secret médical, dossier médical, règles de partage d'informations et hébergement de données). Un règlement type est aussi prévu pour les systèmes d'informations aux termes de l'article 11 de la loi informatique et libertés dans sa rédaction issue du projet de loi.

D'une façon générale, ne sont pas dans le périmètre du chapitre IX tous les traitements liés aux soins (logiciels des professions, hôpitaux…) ainsi que ceux de l'assurance maladie. Cette catégorie couvre par exemple les traitements de données par les médecins pour le suivi médical de leurs patients, les traitements mis en œuvre dans les établissements de santé par les médecins responsables de l'information médicale, les traitements fondés sur le consentement express des personnes concernés (comme les applications de santé à usage individuel).

2. Le traitement des données relevant du chapitre IX

Pour les données relevant du chapitre IX, le principe est la déclaration de conformité à un référentiel ou une méthodologie de référence, l'autorisation accordée par la CNIL demeurant l'exception. Le texte prévoit aussi la possibilité de prendre un règlement type, qui, en droit, ne se limiterait pas aux seuls systèmes d'information, dans le cadre fixé par l'article 11. Les traitements relevant du

chapitre ont finalité commune l'intérêt public mais ne doivent pas aboutir à la ré-identification des personnes.

Le processus diffère toutefois selon les cas de figure :

a) Les traitements aux fins de recherche, d'études ou d'évaluation

Lorsque les traitements concernent les finalités de recherche, d'études ou d'évaluation, il convient de combiner la lecture des sections 1 et 2 du chapitre IX.

La section 1 regroupe des règles communes qui sont donc applicables aux traitements de données de santé (finalité d'intérêt public, règlement type de l'article 11 précité, principe de l'autorisation par la CNIL, principe du silence gardé par la CNIL pendant deux mois vaut acceptation, saisine par la CNIL et auto-saisine de l'Institut national des données de santé (INDS) sur l'intérêt public lorsque la recherche n'implique pas la personne humaine, dispositions relatives aux mineurs).

La section 2 prévoit une procédure spécifique à ce type de traitement : la procédure allégée demeure le principe et se caractérise par la conformité à des « *méthodologies de référence* ». L'autorisation par la CNIL demeure l'exception et fait intervenir l'avis du comité de protection des personnes (CPP) si les recherches impliquent les personnes humaines, le comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES) pour les recherches n'impliquant pas la personne humaine.

Pour le ministère de la santé, le règlement type ne présente pas d'intérêt s'agissant des traitements aux fins de recherche.

b) Les autres traitements ne relevant ni de la section 2, ni des dérogations prévues par la section 1

Le principe demeure la procédure allégée *via* la déclaration de conformité à des référentiels et le respect des règlements types prévus par l'article 11. L'autorisation par la CNIL demeure l'exception.

● Les traitements ne demandant pas d'autorisation sont :

– les jeux de données de santé présentant un faible impact sur la vie privée ;

– les traitements pour lesquels une déclaration de conformité aux référentiel et règlement type est effectuée. Relèveraient de ce cas de figure les traitements des données de santé par messagerie mis en œuvre par les professionnels et établissements de santé et les professionnels du secteur médico-social habilités à cet effet par la loi.

● Les traitements de données susceptibles de relever du régime d'autorisation. Il peut s'agir, par exemple, des traitements liés à la pharmacovigilance.

En relèveraient aussi les traitements consistant à constituer un entrepôt de données. La section 1 couvre en effet l'hypothèse des traitements dont les finalités de recherche ne sont pas encore identifiées et qui nécessitent un régime de protection particulier. Dans ce cadre, le texte prévoit une évolution du rôle de l'INDS qui sera amené à se prononcer sur l'intérêt public de ces traitements, soit sur saisine par la CNIL soit sur auto-saisine. Ce cadre permettrait de couvrir le cas des courtiers en données *(data brokers)*.

ANNEXE 2
LISTE DES PERSONNES AUDITIONNÉES PAR LA RAPPORTEURE

(par ordre chronologique)

- **Association française des correspondants à la protection des données à caractère personnel (AFDCP) – M. Paul-Olivier Gibert**, président et **M. Nicolas Samarcq**, administrateur et responsable du groupe de travail « données de santé », **Mme Marie Noelle Sehabiague,** administratrice, et **M. Moufid Hajjar,** administrateur

- **Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) – Mme Véronika Levendof**, responsable du département juridique, **Mme Gildine Croizé**, responsable de la mission CNIL, et **M. Stéphane Naux**, conseiller juridique auprès du directeur de la stratégie

- **Algorithm Data Ethics Label (ADEL) – M. Jérôme Béranger**, co-fondateur et *chief scientific officer*, chercheur associé à l'UMR 1027 / Inserm à l'Université de Toulouse, **M. Conrad Painvin**, directeur marketing et administratif, **Mme Lina Williatte**, avocate au Barreau de Lille, professeure de droit à l'Université catholique de Lille, membre du comité scientifique, et **M. Jérôme Fortineau**, expert Label Éthique

- **Institut national des données de santé (INDS) – Mme Dominique Polton**, présidente, et **M. Thomas Duong**, conseiller juridique

- **Fédération nationale de la mutualité française (FNMF)**(*)**– M. Albert Lautman,** directeur général**, Mme Pascale Fassinotti,** responsable adjointe du service juridique et fiscal**,** et **Mme Meriem Bouchefra,** chargée d'affaires publiques

- **Institut national de la santé et de la recherche médicale (INSERM) – M. Yves Lévy**, président-directeur général, **Mme Claire Giry**, directrice générale déléguée, et **Mme Frédérique Lesaulnier**, responsable de la conformité en matière de protection des données

- **Commission nationale de l'informatique et des libertés (CNIL) – M. Jean Lessi**, secrétaire général, **M. Thomas Dautieu**, directeur adjoint de la direction de la conformité, et **Mme Tiphaine Havel**, conseillère pour les questions parlementaires et institutionnelles

- **Association Droit à l'Oubli Numérique – M. Ludovic Broyer,** Fondateur/Dirigeant d'IProtego

➢ **Fédération française de l'assurance (FFA)**(*) **– M. Philippe Poiget**, délégué général, **M. François Rosier**, directeur adjoint et **M. Jean-Paul Laborde**, directeur des affaires parlementaires

➢ **Centre technique des institutions de prévoyance (CTIP)**(*) **– M. Jean Paul Lacam**, délégué général, **Mme Mercier-Pariente**, directrice juridique, et **Mme Miriana Clerc**, directrice des relations institutionnelles

➢ **Ministère de la Santé – M. Jean-Marc Aubert**, directeur de la direction de la recherche, des études, de l'évaluation et des statistiques (DREES), **Mme Mylène Girard**, cheffe de la mission d'accès aux données de santé à la DREES, **M. Philippe Ranquet,** directeur des affaires juridiques, **M. Arnaud Deloffre,** chef des pôles à la direction des affaires juridiques, et **M. François Godineau,** chef de projet à la direction de la sécurité sociale

➢ **Syndicat National de l'Industrie des Technologies Médicales (SNITEM) – M. Gabriel Daubech**, responsable des affaires publiques, et **Mme Lucile Blaise**, administratrice du SNITEM et présidente de RESMED

(*) *Ce représentant d'intérêts a procédé à son inscription sur le registre de la Haute Autorité pour la transparence de la vie publique s'engageant ainsi dans une démarche de transparence et de respect du code de conduite établi par le Bureau de l'Assemblée nationale.*