Régulation juridique de la “ médecine numérique ” : évolutions, enjeux et défis de l’utilisation des données de Santé

Céline Gauthier-Maxence

Régulation juridique de la « médecine numérique » : évolutions, enjeux et défis de l'utilisation des données de Santé

Résumé : Cet article explore l'évolution du cadre juridique encadrant la médecine numérique en France et dans l'Union européenne. Partant des bases posées par la loi "Informatique et Libertés" de 1978 jusqu'au Règlement Général sur la Protection des Données (RGPD), l'article examine comment le droit s'adapte aux défis posés par la collecte et le traitement des données de santé, notamment face aux avancées de l'intelligence artificielle et des big data. Le texte souligne les enjeux éthiques et de souveraineté des données, ainsi que les lacunes des régulations actuelles. Il propose des perspectives d'amélioration pour une gouvernance plus éthique et cohérente de la médecine numérique.

Mots clés : RGPD ; Données de santé ; CNIL ; Souveraineté numérique ; IA ; Régulation juridique

Auteur : Céline Gauthier-Maxence

Introduction

La bioéthique a vu le jour en 1945 dans un contexte difficile, marqué par la révélation des pratiques expérimentales inhumaines menées par des chercheurs nazis sur des populations vulnérables, sans aucun consentement, en violation manifeste de la dignité humaine et de l'intégrité corporelle. Ces actes ont été jugés par le tribunal international de Nuremberg [1], où les responsables ont été condamnés au nom du respect de l'être humain. Le « Code de Nuremberg » a alors établi la première barrière éthique. Avec le développement de la recherche médicale et la définition des droits des patients, la bioéthique a progressivement instauré un ensemble de régulations strictes pour encadrer cette évolution, en s'assurant qu'elle serve toujours le bien-être des individus. Le principe fondamental adopté est la primauté de la personne, dont la dignité est considérée comme indivisible, non mesurable, non négociable, et prévalant sur les intérêts de la science et de la société. En cas de conflit, les « *intérêts de l'individu devraient primer sur le seul intérêt de la science ou de la* société »[2].
Pour éviter les dérives et une éventuelle implosion, la « médecine numérique » est encouragée à suivre la voie de la bioéthique. On lui demande avec insistance de s'ouvrir aux questions de régulation juridique. De nombreux experts réclament une intervention du droit, et les citoyens curieux et avertis appellent également à des régulations[3]. Dans ce contexte, le droit est donc attendu, bien qu'il soit déjà présent. L'état du droit existant s'appuie sur la régulation de la collecte, du traitement et de l'utilisation des données personnelles fournies par les patients pour les besoins de la recherche et l'amélioration des pratiques de soin. Des systèmes de régulation qui concernent les données personnelles en général, mais aussi les

données médicales, ont été mis en place ; systèmes qui seront analysés dans le présent article. Cet ensemble de régulations s'applique aux « données massives », ou *big data*, hébergées à grande échelle dans les hôpitaux ou les centres agréés. Il s'applique également au stockage de données sanitaires dans les cabinets médicaux du secteur libéral, à plus petite échelle.
Les hôpitaux et les établissements de santé voient croître un nombre important de bases de données médicales. Chercheurs et acteurs du secteur médical et social exercent des pressions pour faciliter la circulation maximale des données, au nom de l'avancement des pratiques médicales et de la recherche. Ces bases de données ne sont pas des entités autonomes flottant librement ; il a donc fallu les ancrer et encadrer par des réglementations strictes. Les dispositions juridiques actuelles agissent de manière dialectique. D'un côté, elles définissent les règles de structuration des bases de données en se fondant sur des critères précis : finalité de la collecte, nature des données, population concernée, destinataires autorisés à y accéder, et durée de conservation. De l'autre, elles réaffirment systématiquement les droits des individus relatifs à leurs données, cherchant à établir un équilibre entre des intérêts complémentaires, mais potentiellement opposés : d'une part, les intérêts institutionnels relatifs à l'exploitation des données de santé, et d'autre part, les droits des personnes, qui, selon un principe de bioéthique bien établi, prévalent toujours sur les intérêts scientifiques et sociétaux. Mais cette approche multitâche est-elle réellement efficiente et convaincante ? Le cadre de régulation a évolué au fil du temps et se décline en trois modèles : le modèle initial de 1978, le modèle institutionnalisé en faveur des politiques de santé publique de 2016 (I), et le modèle élargi aux pays de l'Union européenne (II). Mais ces modèles juridiques présentent effectivement des failles évidentes auxquelles il faudra tôt ou tard se confronter (III).

I. Le cadre juridique initial de la médecine numérique française, un cheminement par étapes

A. Les fondements juridiques de la régulation des données de santé

La loi du 6 janvier 1978, dite "Informatique et Libertés"[4], a instauré un cadre légal pour la protection des données personnelles en France, bien avant l'avènement du RGPD. Cette loi vise à encadrer la collecte, le traitement et la conservation des données afin de protéger la vie privée des personnes. Elle est générale et concerne indirectement les données de santé. Elle prévoit des prérogatives spécifiques pour les individus concernant leurs informations personnelles, ainsi que des obligations pour les responsables de traitement, sous la surveillance de la Commission Nationale de l'Informatique et des Libertés (CNIL). Avant la mise en œuvre d'un fichier de données, le responsable du traitement doit effectuer une déclaration préalable auprès de la CNIL. Cette démarche vise à s'assurer que le traitement des données respecte les dispositions légales. Cette déclaration doit inclure plusieurs informations clés (article 19) ; l'identification de l'entité ou de la personne responsable du traitement des données, la nature des données collectées et finalités du traitement, l'identification des individus dont les données seront traitées, les entitées ou personnes ayant accès aux informations collectées, la période pendant laquelle les données seront conservées, les mesures mises en place pour protéger les données contre tout accès non autorisé, altération ou perte, et les dispositifs garantissant la protection des informations personnelles, comme la pseudonymisation ou l'anonymisation des données.

En outre, les individus disposent de plusieurs droits fondamentaux en vertu de la loi du 6 janvier 1978. Les technologies informatiques doivent être utilisées au bénéfice de tous les citoyens. Elles ne doivent en aucun cas nuire à l'intégrité de la personne, aux droits fondamentaux, à la protection de la vie privée, ni aux libertés, qu'elles soient individuelles ou collectives (article 1). Chacun a le droit d'être informé des données et des raisonnements employés dans les traitements automatisés qui produisent des effets à son encontre, ainsi que de les contester (article 3). Dans la continuité, toute personne a le droit d'être informée de l'existence d'un fichier contenant des informations la concernant. Cette transparence est essentielle pour assurer la confiance et le contrôle des personnes sur leurs données. Les individus peuvent accéder au contenu des informations les concernant et, le cas échéant, demander la rectification des données inexactes ou incomplètes (articles 22, 25, 26, 27, 34, 45). Les personnes peuvent s'opposer, pour des motifs légitimes, à l'enregistrement ou au traitement de leurs données personnelles. Ce droit est essentiel pour limiter l'utilisation des données dans des contextes non souhaités par les individus. Le droit de communication permet aux personnes concernées d'obtenir une copie de leurs données dans un format clair et compréhensible, conforme à leur enregistrement dans le système de traitement. Les individus peuvent demander à la CNIL de vérifier l'existence d'autres fichiers les concernant. Cette demande s'appuie sur la liste des traitements de données gérée par la CNIL, garantissant un contrôle sur la dissémination des informations personnelles (article 6).
La CNIL, également créée par cette loi, est une autorité administrative indépendante. Elle a pour mission de veiller à la protection des données personnelles et de garantir le respect des libertés individuelles. La CNIL a le pouvoir de contrôler la conformité des traitements de données avec les obligations légales. Elle peut également émettre des recommandations, des mises en demeure, et des sanctions administratives en cas de manquements. La CNIL joue également un rôle essentiel dans l'information du public et des professionnels sur leurs droits et obligations. Elle publie régulièrement des guides et des avis pour aider à la mise en conformité avec la législation en vigueur[5].
Enfin, en cas d'infraction, la loi prévoit des sanctions pénales pour toute violation des dispositions relatives à la collecte, la divulgation ou l'utilisation abusive des données personnelles. Ces infractions incluent l'atteinte à l'intimité de la vie privée des personnes par des traitements non conformes (articles 41 à 44). Ces sanctions pénales incluent l'emprisonnement, pouvant aller de 6 mois à 5 ans en fonction de la gravité de l'infraction, et l'amende de 2 000 à 20 000 francs, selon la nature et la gravité de la violation. En cas de contentieux, le juge peut intervenir pour sanctionner les infractions et protéger les droits des personnes concernées. Les décisions de justice peuvent également établir des dommages et intérêts pour les victimes d'un traitement illicite de leurs données.

La loi du 6 août 2004[6], qui intègre dans le droit français les dispositions de la directive européenne 95/46 CE[7], apportera de nombreuses modifications à la loi Informatique et Libertés. Ces nouvelles dispositions concernent la déclaration des fichiers et précisent la liste des données dont la collecte est interdite. En effet, la Loi du 6 janvier 1978 proscrivait le traitement des données qualifiées de sensibles[8], en énonçant une liste des catégories concernées. Mais les informations relatives à la santé ne faisaient pas partie de cette liste initiale. Ce n'est qu'avec la modification apportée par la Loi du 6 août 2004 qu'elles y ont été intégrées. Le modèle présenté de manière synthétique servira d'infrastructure pour les modèles qui suivront.

B. La loi du 26 janvier 2016 ; le modèle institutionnalisé de gestion des données de santé

Depuis 2016, la France dispose d'une base de données publiques exceptionnellement riche dans le domaine de la santé. Cette base a été créée par la loi du 26 janvier 2016[9], dite loi de modernisation du système de santé, impulsée par Marisol Touraine, alors ministre de la Santé. L'objectif est la mise en place d'un « système national des données de santé » (SNDS). La référence au socle de base établi par la loi Informatique et Libertés est nette. La même architecture est adoptée : celle-ci proposait un modèle standard, celle-là crée une base de données conforme à ce standard.
La loi de 2016 interdit l'utilisation des données contenues dans ce fichier à des fins de promotion de produits de santé, ainsi qu'à des fins d'exclusion de garanties dans les contrats d'assurance ou de modification des cotisations et des primes d'assurance.

Le modèle institutionnalisé repose donc sur le Système National des Données de Santé (SNDS), régulé par la Caisse nationale de l'assurance maladie des salariés (CNAM). Ce dispositif, régi par la loi du 26 janvier 2016 et les décrets subséquents, vise à structurer et à encadrer l'accès aux données de santé dans un but d'intérêt public, tout en assurant la protection des droits des personnes concernées. Ce modèle est soutenu par un cadre juridique strict, incluant des normes de confidentialité et des procédures de contrôle.
Concernant la responsabilité et la gestion des données, la CNAM est le principal responsable de la gestion du SNDS. Dans le cadre d'une convention, d'autres entités, comme l'Inserm, peuvent être autorisées à effectuer des extractions de données pour des recherches, des études ou des évaluations des pratiques de soin. Le responsable du traitement doit garantir la conformité du dispositif aux obligations légales, y compris la pseudonymisation des données. Les données enregistrées dans le SNDS ne contiennent pas d'informations directement identifiantes, telles que les noms, prénoms, numéros de sécurité sociale ou adresses postales. Elles comprennent cependant des pseudonymes, le sexe, le mois et l'année de naissance, le lieu de résidence et des informations médicales (prestations fournies, arrêts de travail, etc.). Les données relatives aux organismes de santé incluent les prestations et prises en charge associées à chaque bénéficiaire. Ce système intègre les bases de données préexistantes dispersées (assurance maladie, établissements de santé, Inserm, mutuelles) et est de nature principalement administrative. Le SNDS vise à améliorer la connaissance des prises en charge médicales, à élargir le champ des recherches, des études et des évaluations dans le domaine de la santé publique. Ce système soutient l'évolution des politiques de santé en fournissant un cadre structuré pour l'analyse des données de santé, dans un objectif d'intérêt collectif. L'accès permanent aux données est accordé à certains services publics, tels que la Direction générale de la santé, les agences régionales de santé, l'Agence nationale de sécurité du médicament, l'Inserm, et d'autres institutions de recherche publique (Art. R.1461-12 du Code de la santé publique). Pour d'autres entités, notamment les organismes privés, l'accès est soumis à l'autorisation de la CNIL, qui doit vérifier l'intérêt public de la demande. Les données sont conservées pendant une durée de 19 ans, puis archivées pour une période de 10 an supplémentaire. Ce délai est conforme aux exigences légales en matière de conservation des données, permettant un suivi à long terme des pratiques de soin et des politiques de santé.
Concernant les dispositifs de sécurité et la protection des données, un référentiel spécifique, basé sur la loi du 26 janvier 2016 et l'arrêté de mars 2017, encadre la sécurité des données. Il prévoit des mesures de pseudonymisation, d'authentification des utilisateurs, et de traçabilité

des accès et des actions. La CNAM doit veiller à la confidentialité, à l'intégrité et à la disponibilité des données, en garantissant leur sécurité face aux risques de perte, d'altération ou d'accès non autorisé. La pseudonymisation est l'une des mesures principales pour la protection de la vie privée des personnes. Chaque individu se voit attribuer un code alphanumérique unique, ne permettant pas de le rattacher directement à son identité civile. Ce dispositif est complété par des mesures d'authentification et de traçabilité, assurant un contrôle strict des actions effectuées sur les données.
Enfin, les personnes concernées doivent être informées de la constitution du SNDS et des possibilités de réutilisation de leurs données à des fins de recherche. Cette information est accessible sur les sites internet des hôpitaux ou des organismes d'assurance maladie. Les personnes disposent d'un droit d'accès, de rectification et d'opposition à l'égard de leurs données. Toutefois, ces droits ne peuvent s'exercer pour les traitements de données nécessaires à l'exercice des missions des services publics. En cas de traitement à des fins de recherche, l'information doit être fournie par le responsable de l'étude ou de l'établissement de santé concerné.
Le contrôle de l'utilisation des données s'effectue a posteriori, principalement par le biais d'audits externes. La CNIL, en tant qu'autorité de contrôle, est toujours chargée de surveiller l'application des mesures légales et de sanctionner les violations. En cas de non-conformité, les responsables de traitement peuvent se voir infliger des sanctions administratives, incluant des amendes conséquentes. L'accès aux données par les entreprises productrices de produits de santé ou les assureurs est soumis à des conditions strictes. Ils doivent soit passer par un organisme de recherche indépendant, soit démontrer que les modalités d'accès respectent les finalités légitimes prévues par la loi. Toute recherche impliquant la personne humaine nécessite un avis favorable d'un comité de protection des personnes avant sa mise en œuvre.

Finalement, le législateur a poursuivi un double objectif : créer un outil de travail plus logique et accessible pour les professionnels de santé, tout en assurant la protection des données personnelles collectées. Cela permet d'offrir une information précise sur la santé au niveau territorial, de recenser l'offre de soins, d'évaluer les politiques de santé, de mieux comprendre les dépenses et de garantir la sécurité sanitaire. Par ailleurs, cet outil permet aux médecins d'avoir une vision d'ensemble des problématiques et d'apporter une réponse plus adaptée au contexte local en cas de hausse d'une pathologie, notamment par le biais de campagnes de sensibilisation. Il s'agit d'une base de données d'envergure, avec une structure bien définie et une orientation résolument administrative. La loi de 2016 qui la sous-tend repose sur le regroupement de structures existantes, favorisant ainsi l'accès à l'information et sa diffusion efficace aux acteurs concernés. Elle constitue une loi de fusion, intégrant le rapport dialectique précédemment mentionné : la circulation des données de santé et la sécurisation des droits des patients.

II. Le modèle ouvert sur l'Union européenne : le RGPD et la Loi du 20 juin 2018

A. Un cahier des charges entre évolutions et révolutions

Dans les pays de l'Union européenne, on trouve des dispositifs de régulation des données personnelles qui sont plus ou moins similaires. Sous l'influence des nouvelles technologies de communication, de la diversification des fichiers de santé nominatifs et des échanges

transnationaux, les acteurs européens responsables du domaine de la santé ont adopté une démarche de concertation. Ils ont comparé les différents systèmes pour travailler à l'élaboration d'un référentiel commun, avec pour objectif d'harmoniser les règles et les pratiques. Ainsi, ils ont publié le « Règlement général sur la protection des données » (RGPD) le 27 avril 2016, qui est entré en application le 25 mai 2018[10]. Ce règlement propose un modèle standard pour la gestion des données personnelles en général. Les données sanitaires sont concernées au même titre que les autres, avec des dispositions spécifiques. Les différents pays de l'Union ont dû transposer ce standard dans leur propre réglementation. En France, cela a été fait par la loi du 20 juin 2018[11]. Ce dispositif s'applique aussi bien aux hôpitaux qu'aux structures de soins et aux praticiens libéraux dans les cabinets médicaux.
Cette nouvelle réglementation européenne élargit la liste des données sensibles en y incluant les données génétiques et biométriques. Bien que le traitement des données de santé soit permis, cela se fait par le biais d'une dérogation au principe général d'interdiction. Il s'agit d'une autorisation exceptionnelle, similaire à ce qui existait en bioéthique pour la recherche sur l'embryon[12] avant qu'une loi ultérieure n'accorde une autorisation directe[13]. Cela revient finalement à maintenir une interdiction de principe pour sa valeur symbolique, tout en accordant une dérogation pour des raisons pratiques.
Le dispositif adopte une démarche dialectique qui oppose les droits des individus à l'influence des *big data* et des algorithmes. Ce cadre réglementaire se veut démocratique. Il n'est plus nécessaire de solliciter une autorisation auprès de la CNIL. Les acteurs doivent désormais concevoir eux-mêmes leur dispositif en tenant compte des exigences du standard, des règles de base à portée européenne, tout en respectant les spécificités locales.
Chaque pays de l'UE se doit de mettre en place une autorité de contrôle exerçant une supervision a posteriori. Les responsables des dispositifs sont notamment tenus d'assurer un suivi et une réévaluation constants des adaptations nécessaires pour s'adapter aux évolutions technologiques et maintenir l'efficacité des systèmes de sécurité face aux divers risques : piratage, vol de données, détérioration, les pratiques des hackers ou pirates ayant souvent une longueur d'avance sur les mesures de défense techniques. Le système de protection inclut les moyens déployés pour protéger la personne et ses données personnelles, notamment par le recours à l'anonymisation ou à la pseudonymisation.
Le RGPD reprend également de nombreux principes déjà présents dans la loi « Informatique et Libertés » : consentement, droit à l'oubli, suppression des informations au-delà d'un certain délai. Indéniablement, le trait majeur est le renforcement des droits de la personne en parallèle avec le développement des *big data* sanitaires. De plus, l'enregistrement des données de santé et leur traitement sont interdits en dehors de la sphère médicale (Article 6-1), sauf dérogations sous couvert de l'accord libre et explicite des patients concernés.

Plus précisément, le RGPD repose sur plusieurs principes clés énoncés à l'article 5 ; huit d'entre eux sont à relever, nécessairement. Le principe de licéité et de loyauté, selon lequel les traitements de données doivent correspondre aux informations fournies au patient, qui conditionnent son consentement éclairé et l'exercice de ses droits. Le principe de transparence, selon lequel les individus ont le droit de connaître les finalités du traitement et d'identifier le responsable du système. Le principe de limitation des finalités, selon lequel les données doivent être collectées pour des finalités précises, explicites et légitimes, et ne doivent pas être utilisées de manière incompatible. Le principe de minimisation des données qui implique que les informations recueillies doivent être limitées au strict nécessaire en rapport avec les finalités du traitement. Le principe d'exactitude des données, qui induit que

les données doivent être tenues à jour et corrigées ou supprimées si nécessaire. Le principe de limitation de la durée de conservation ; les données personnelles ne doivent pas être conservées plus longtemps que nécessaire pour les finalités pour lesquelles elles ont été collectées. Le principe de sécurité et de confidentialité implique le responsable du traitement doit assurer une protection adéquate contre tout traitement illicite ou perte accidentelle de données, et mettre en œuvre des mesures techniques et organisationnelles appropriées. Enfin, le principe de responsabilité qui impose au responsable du traitement de pouvoir démontrer sa conformité à l'ensemble de ces principes, notamment par la tenue d'un registre des traitements et la réalisation d'analyses d'impact, conformément aux articles 5-1 et 5-2 du RGPD.

L'article 30 du RGPD impose la tenue d'un registre des traitements de données à tous les organismes, qu'ils soient publics ou privés. Ce document, qui recense de manière exhaustive les traitements effectués, constitue un outil de gouvernance et de démonstration de la conformité au RGPD. Il doit inclure les finalités des traitements, les catégories de personnes concernées, les destinataires des données, les éventuels transferts vers des pays tiers ou des organisations internationales, les durées de conservation des données, un descriptif des mesures de sécurité mises en œuvre.

Une analyse d'impact est requise lorsque le traitement des données présente un risque élevé pour les droits et libertés des personnes concernées, par exemple dans les cas de traitements de données de santé sensibles ou concernant des populations vulnérables. Elle vise à identifier et à atténuer les risques associés[14]. Le responsable du traitement, personne morale ou physique, détermine les finalités et les moyens du traitement. Ce rôle inclut la mise en œuvre des mesures techniques et organisationnelles nécessaires pour garantir la conformité au RGPD. Lorsqu'un traitement implique une surveillance à grande échelle, comme dans le cadre de réseaux de professionnels de santé ou de dossiers médicaux partagés, la désignation d'un Délégué à la Protection des Données (DPO) est obligatoire. Le DPO, qu'il soit interne ou externe, conseille de manière indépendante le responsable du traitement sur les obligations légales. Les personnes concernées doivent être informées de manière claire, transparente et compréhensible. L'information doit inclure l'identité du responsable du traitement, les coordonnées du DPO, les finalités du traitement, les destinataires des données, la durée de conservation, et les droits d'accès, de rectification, de limitation ou d'opposition au traitement.

B. Droits des personnes sur les données médicales personnelles dans le RGPD

Les droits des personnes sur leurs données médicales personnelles, inscrits dans le cadre juridique européen, visent à garantir la maîtrise des individus sur leurs données tout en tenant compte des spécificités liées à leur nature médicale. Les personnes doivent être informées de manière claire et concise sur les données collectées les concernant, les finalités de leur utilisation, la durée de conservation, et les éventuels destinataires des informations. Déjà existant, ce droit se voit renforcé par le RGPD. Les personnes concernées peuvent désormais obtenir davantage d'informations, telles que la source des données lorsque celles-ci n'ont pas été collectées directement auprès d'elles, les détails sur un éventuel profilage, ainsi que les garanties appliquées en cas de transfert de données en dehors de l'Union européenne. Conformément à l'article 16 du RGPD, les individus peuvent demander la rectification de leurs données personnelles si celles-ci s'avèrent inexactes ou incomplètes. Ce droit leur permet de s'assurer que les informations les concernant sont correctes et à jour. Le droit à l'oubli,

renforcé par l'article 17, permet aux personnes de demander l'effacement de leurs données personnelles lorsque celles-ci ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées, ou si la personne retire son consentement. Ce droit s'applique également en cas d'opposition au traitement ou si le traitement devient illicite. Il inclut également le déréférencement des informations sur les moteurs de recherche, garantissant ainsi une protection accrue de la vie privée. L'article 21 reconnaît le droit à toute personne de s'opposer, pour des motifs légitimes, à un traitement de données. Toutefois, ce droit n'est pas absolu ; le responsable du traitement peut justifier la poursuite du traitement s'il prouve qu'il existe un motif légitime supérieur. Introduit par l'article 18, ce droit permet de « geler » temporairement les données, c'est-à-dire de les conserver sans les traiter, dans certains cas spécifiques : contestation de l'exactitude des données, nécessité de rectification, traitement illicite, ou encore action en justice. Ce mécanisme de limitation offre un cadre de protection supplémentaire pendant les périodes de litige ou de vérification. Nouveau droit introduit par le règlement, le droit à la portabilité des données constitue un prolongement du droit d'accès. Les personnes peuvent récupérer les données fournies à un responsable de traitement et les transférer à un autre, facilitant ainsi la circulation des informations tout en préservant le contrôle de l'individu sur ses données. L'article 13 introduit un nouveau droit concernant le profilage, qui consiste à analyser et croiser des données personnelles pour associer l'individu à une catégorie spécifique. Ce processus, bien que légitime, doit être précédé d'une étude d'impact, et la personne concernée doit en être informée. Aucune décision significative ne peut être prise uniquement sur la base d'un profilage automatisé, garantissant ainsi la prise en compte des spécificités individuelles dans le traitement des données.

C. Dispositifs de contrôle et sanctions du RGPD

Le RGPD a également instauré des dispositifs de contrôle rigoureux et des sanctions pour assurer le respect des règles relatives à la protection des données personnelles. En France, c'est la CNIL qui est chargée de veiller à l'application de ces dispositions. Les autorités de contrôle, telles que la CNIL en France, sont des entités indépendantes mandatées par chaque État membre de l'Union européenne. Elles disposent de pouvoirs d'enquête et peuvent imposer des mesures coercitives en cas de non-respect des obligations du RGPD. Le rôle de ces autorités est crucial pour assurer la conformité des traitements de données au sein de leur juridiction respective. La CNIL agit comme un guichet unique en matière de protection des données. Elle est l'interlocuteur principal pour tous les établissements du responsable de traitement, y compris ceux situés en dehors de l'UE, lorsque des données personnelles sont transférées hors du territoire européen. Les décisions de la CNIL sont applicables dans toute l'Union européenne, facilitant ainsi le recours des personnes résidant en France. Ce mécanisme vise à harmoniser les pratiques et à renforcer la protection des droits des individus à l'échelle européenne.

Les sanctions pour non-conformité au RGPD suivent un processus graduel, adapté à la gravité des infractions. En cas de première infraction mineure, la CNIL peut émettre un simple avertissement pour inciter à la mise en conformité. Si l'avertissement reste sans effet, une mise en demeure est prononcée, obligeant le responsable de traitement à se conformer dans un délai imparti. En cas de non-conformité persistante, la CNIL peut ordonner la suspension des transferts de données, notamment vers des pays tiers ne garantissant pas un niveau de protection adéquat. Si le traitement des données est illicite ou n'est plus nécessaire, la CNIL peut exiger leur effacement. Si le responsable de traitement persiste dans la non-conformité,

la CNIL peut infliger des amendes administratives. Celles-ci sont calculées en fonction de la gravité de l'infraction et peuvent atteindre jusqu'à 4 % du chiffre d'affaires annuel mondial de l'entreprise, ou 20 millions d'euros, le montant le plus élevé étant retenu. Ce dispositif vise à dissuader les infractions et à garantir la protection effective des données personnelles. Les victimes d'une violation de leurs données personnelles peuvent obtenir réparation en engageant une action en justice pour réclamer des dommages et intérêts. Elles peuvent se tourner vers les juridictions compétentes pour obtenir une indemnisation proportionnelle au préjudice subi. Les décisions de la CNIL peuvent faire l'objet d'un recours devant le Conseil d'État. Un cas emblématique est celui de la condamnation de Google, en janvier 2019, à une amende de 50 millions d'euros pour des irrégularités dans le recueil des données personnelles. C'était la première fois qu'un géant du web était sanctionné dans le cadre du RGPD[15]. Toutefois, le Conseil d'État a annulé partiellement cette décision le 19 juin 2020[16], démontrant l'importance du cadre judiciaire dans la régulation des sanctions administratives. En somme, la loi de 2018 incarne une législation ouverte, en accord avec l'idée d'une république numérique. Il appartient aux acteurs concernés de prendre leurs responsabilités, sous réserve d'un contrôle a posteriori déjà évoqué. Les citoyens, notamment les patients, doivent être informés de leurs droits et être en mesure de les défendre, le cas échéant, par le biais d'actions judiciaires collectives menées par des associations ou par l'intervention de la CNIL, a posteriori.

En ce qui concerne la recherche, les interactions avec la CNIL se sont simplifiées. Les données, collectées dans le cadre d'un suivi médical, le sont par les personnes en charge de ce suivi et uniquement pour leur usage exclusif. Dans cette situation, aucune formalité n'est requise auprès de la CNIL, mais les modalités de traitement doivent être consignées dans le registre de suivi. Pour les recherches multicentriques, le cadre juridique est allégé. Le responsable doit être capable de démontrer que le traitement envisagé est conforme à l'un des référentiels élaborés par la CNIL, ce qui nécessite une déclaration préalable de conformité auprès de celle-ci. En matière de recherche, les données doivent impérativement être protégées, soit par anonymisation, soit par pseudonymisation. Le responsable adopte alors une logique de responsabilité, sans contrôle préalable de la CNIL, conformément à l'esprit du RGPD. Les documents sont enregistrés dans le registre de suivi, en tant que preuve de la confidentialité et de la sécurité exigées.
Toutefois, une autorisation est requise lorsque le traitement présente un intérêt public (par exemple, en ce qui concerne les normes de qualité et de sécurité des médicaments). La même rigueur s'applique aux traitements automatisés destinés à des recherches générales en santé ou à l'évaluation des pratiques de soins ou de prévention[17].

III. Limites et perspectives de la régulation juridique de la médecine numérique

A. Les limites du cadre juridique actuel

Le cadre juridique actuel de la médecine numérique, bien qu'avancé, présente des lacunes significatives. Tout d'abord, la complexité du cadre législatif, découlant de l'enchevêtrement des lois nationales et européennes, rend difficile la compréhension et l'application des normes par les professionnels de santé. Le RGPD, par exemple, impose des obligations strictes en matière de protection des données personnelles, mais son application aux données de santé,

qui sont particulièrement sensibles, manque de précisions claires et opérationnelles pour les praticiens et les chercheurs[18].

Ensuite, le cadre juridique ne parvient pas à anticiper efficacement les évolutions technologiques rapides, notamment l'introduction de l'intelligence artificielle (IA) en médecine. L'OMS souligne la nécessité d'une gouvernance robuste, incluant des évaluations rigoureuses des systèmes d'IA, afin de s'assurer de leur sécurité et de leur conformité aux droits humains. Cependant, malgré ces recommandations, l'encadrement juridique de l'IA en santé reste fragmenté et incomplet, surtout en ce qui concerne la transparence des algorithmes et la prévention des biais discriminatoires inhérents aux systèmes d'apprentissage automatique[19].

De plus, les systèmes de régulation actuels, tels que le SNDS en France, malgré leur ambition d'organiser et de centraliser les données médicales, posent des défis majeurs en termes de sécurité et de confidentialité. Le principal enjeu souvent évoqué par les commentateurs est la question de la souveraineté de l'Europe sur ses données de santé. Ces informations constituent un capital de plusieurs milliards de dollars, dans la mesure où elles permettent de développer des médicaments, de nouveaux algorithmes et d'améliorer l'intelligence artificielle, adaptée à chaque situation spécifique. Le risque est d'aboutir à une commercialisation excessive de ce capital santé, voire à l'exploitation des patients. Pour éviter cela, il est indispensable de sécuriser nos données de santé. Il est impératif, en premier lieu, de ne pas confier ces données à des entreprises telles que Google, Apple, Facebook, Amazon ou Microsoft, car leur modèle économique dans un contexte libéral tel que celui des États-Unis repose sur la monétisation de tout, absolument tout. D'autant plus que ces entreprises sont soumises à la législation américaine, notamment le Cloud Act[20]. Lorsque des données, même étrangères, sont stockées dans le cloud de ces entreprises, elles deviennent juridiquement accessibles aux États-Unis[21]. Il est urgent que l'Europe assure sa souveraineté dans la gestion de ses données de santé[22], car le stockage et l'accès à ces dernières par des entreprises non européennes, comme les géants de la tech, restent une menace potentielle pour la protection des droits des patients. Les critiques s'accentuent sur le fait que la France et l'Europe n'ont pas encore mis en place de structures suffisantes pour protéger leurs données de santé contre l'extraterritorialité des lois américaines[23]. A ce titre, le véritable défi du RGPD réside dans la capacité des États membres de l'UE à imposer le respect de cette législation aux entreprises établies en dehors de l'Union, dans des pays n'ayant pas de cadre réglementaire équivalent et ne partageant pas la même culture, notamment les États-Unis.

Enfin, l'application des droits des patients reste une problématique non résolue. Bien que le RGPD confère des droits étendus aux individus sur leurs données personnelles, leur mise en œuvre concrète dans le domaine médical se heurte souvent à des obstacles pratiques. Par exemple, l'exercice du droit à l'effacement des données (le « droit à l'oubli ») est limité lorsqu'il entre en conflit avec des exigences de santé publique ou de recherche médicale. Ces limitations sont perçues comme un frein à la protection des droits individuels face aux impératifs collectifs[24]. Cependant, l'information des populations reste insuffisante pour ce faire et les individus sont souvent la source de leur propre malheur. En effet, le CNOM regrette toutefois le manque de prudence ou l'indifférence de certains citoyens en matière de diffusion de données personnelles. Les citoyens partagent leurs données de santé en grande quantité via diverses applications ou dispositifs connectés. Ces données personnelles peuvent être

collectées par des entités privées, sans contrôle ni régulation, et pourraient être utilisées à d'autres fins, notamment commerciales, que celles initialement prévues par l'utilisateur. Il est probable que les citoyens ne mesurent pas pleinement ces risques, à moins qu'ils ne les considèrent acceptables en contrepartie des services qu'ils utilisent[25].

B. Vers une régulation éthique et globale de la médecine numérique

La régulation de la médecine numérique doit évoluer vers une approche plus globale et éthique, intégrant des principes d'équité, de transparence et de responsabilité. Plusieurs pistes peuvent être envisagées pour renforcer ce cadre.
Tout d'abord, il est crucial de développer des normes éthiques internationales spécifiques à l'IA en santé, au-delà des recommandations actuelles. L'OMS a appelé à la création d'un cadre juridique international pour garantir que les systèmes d'IA soient utilisés de manière éthique et conforme aux droits humains. Cela inclut des obligations de transparence pour les algorithmes d'IA, des mécanismes de responsabilisation pour les développeurs et les utilisateurs, ainsi que des processus rigoureux de validation avant et après la mise en œuvre des technologies dans les soins médicaux[26].
Ensuite, un effort concerté est nécessaire pour améliorer la formation des professionnels de santé sur les questions juridiques et éthiques associées à la médecine numérique. La formation aux spécificités techniques et légales de la télémédecine est indispensable pour une pratique conforme et sécurisée[27]. Cela passe par l'implication active des institutions de formation, des ordres professionnels et des organismes de régulation.

Par ailleurs, la création d'une agence européenne dédiée à la régulation des données de santé et des technologies numériques en médecine pourrait renforcer la souveraineté européenne en matière de protection des données. Cette agence aurait pour mission de coordonner les efforts des États membres, de développer des standards communs, et d'assurer une vigilance accrue face aux menaces de cybercriminalité et de transfert illégal de données. En effet, le projet de l'Espace Européen des Données de Santé (EHDS) a été proposé pour renforcer la souveraineté européenne en matière de protection des données de santé ; il découle de la stratégie européenne pour les données[28]. Il vise à faciliter l'échange sécurisé de données médicales à travers l'UE, en établissant des standards communs et des mécanismes de surveillance contre les cybermenaces. L'EHDS inclut également des consultations publiques pour impliquer les citoyens dans la gestion de leurs données[29]. Enfin, l'implication des citoyens et des patients dans l'élaboration des politiques de régulation est primordiale. Les patients doivent être pleinement informés et consultés sur l'utilisation de leurs données de santé. La promotion de cadres participatifs, où les individus peuvent influencer les décisions sur la gestion de leurs informations, renforcerait la légitimité et l'acceptabilité des régulations mises en place. L'implication des citoyens et des patients dans l'élaboration des politiques de régulation des données de santé est un objectif central du projet de l'EHDS[30]. Ce projet a été approuvé par le Parlement européen en 2024. Il prévoit également des consultations publiques pour assurer que les politiques de gestion des données soient alignées avec les attentes des citoyens et pour renforcer leur légitimité. Les citoyens auront la possibilité d'exercer leurs droits sur leurs données en ajoutant des informations, en corrigeant des erreurs et en limitant l'accès aux professionnels de santé. Cela vise à promouvoir un cadre participatif où les individus peuvent influencer les décisions concernant leurs informations personnelles, améliorant ainsi la transparence et la confiance dans l'utilisation des données

de santé à des fins de recherche et d'innovation. Le projet inclut aussi la création d'autorités de santé numérique dans chaque État membre pour garantir la protection des droits des citoyens, facilitant ainsi une gestion plus efficace et sûre des données de santé à travers l'Europe[31]. En somme, une régulation éthique et globale de la médecine numérique nécessite une coopération accrue entre les acteurs politiques, juridiques, scientifiques et sociétaux. Cela permettrait de garantir un usage des technologies numériques bénéfique pour la société, tout en respectant pleinement les droits et la dignité des patients[32].

Conclusion

Il apparaît que le cadre juridique de la médecine numérique, bien qu'avancé, doit encore évoluer pour répondre aux défis posés par les technologies émergentes, notamment l'intelligence artificielle et les *big data*. L'interaction complexe entre la protection des droits individuels et l'exploitation des données pour le progrès médical nécessite un équilibre délicat. Face aux menaces potentielles, telles que la souveraineté des données et la protection contre les intrusions commerciales, il est impératif d'envisager une régulation plus cohérente et éthique à l'échelle internationale. Le projet de l'Espace Européen des Données de Santé constitue une avancée prometteuse en ce sens. Cependant, il sera crucial d'impliquer davantage les citoyens dans les processus de décision pour renforcer la légitimité des politiques mises en place. L'avenir de la régulation juridique en bioéthique devra donc s'orienter vers une intégration plus harmonieuse entre innovation technologique et respect des droits fondamentaux. En tout état de cause, une évolution prochaine sera déjà à considérer concernant, par exemples, l'application du Digital Operational Resilience Act (DORA)[33] et de l'AI Act[34] en matière de médecine numérique. Le DORA, bien qu'il cible principalement le secteur financier, impose des obligations en matière de résilience numérique qui peuvent toucher indirectement les services financiers des structures de santé, tels que la gestion des factures et des assurances. Le DORA impose l'adoption de cadres de gestion des risques liés aux technologies de l'information, y compris la cybersécurité des systèmes numériques (article 4). Cela peut concerner les systèmes financiers des hôpitaux et autres entités de soins de santé. Il met également l'accent sur la gestion des risques liés aux prestataires tiers, ce qui s'applique aux fournisseurs de services informatiques et de cloud utilisés par les établissements de santé (article 6). En ce qui concerne le futur AI Act[35], il vise à encadrer les systèmes d'intelligence artificielle en fonction de leur niveau de risque. Les systèmes d'IA employés dans le domaine médical, comme pour le diagnostic ou l'aide à la décision clinique, sont considérés comme "à haut risque". Ces systèmes devront respecter des normes strictes de sécurité, de transparence et d'explicabilité (article 8). Par exemple, les IA utilisées pour l'analyse de données médicales devront être conçues de manière à minimiser les biais et à garantir des résultats fiables. Les développeurs et utilisateurs de ces technologies devront prouver leur conformité, notamment en ce qui concerne la gestion des données et la réduction des risques. Cela comprend le besoin de tester les algorithmes afin d'éviter des erreurs susceptibles de mettre en danger les patients. La conformité à ces réglementations sera donc cruciale pour garantir la protection des données des patients et la continuité des soins, tout en évitant de lourdes sanctions et en répondant aux exigences éthiques et légales de plus en plus strictes.

Références :

[1] « Procès des grands criminels de guerre devant le Tribunal Militaire International, Nuremberg, 14 novembre 1945-1er octobre 1946 », Texte officiel en langue française, Édité à Nuremberg, Allemagne, 1947, https://www.legal-tools.org/doc/512713/pdf/

[2] Déclaration universelle sur la bioéthique et les droits de l'homme, Unesco, 19 octobre 2005.

[3] CCNE, Rapport de synthèse, Bioéthique, États généraux.

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

[5] Qu'est-ce que la CNIL ? : https://www.cnil.fr/fr/cnil-direct/question/la-cnil-cest-quoi

[6] Loi n° 2004-800 du 6 août 2004 relative à la bioéthique, JORF n°182 du 7 août 2004

[7] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel n° L 281 du 23/11/1995 p. 0031 - 0050

[8] « Données numériques de santé : entre enjeux médicaux, technologiques et juridiques », Vie publique, publié le 6 juin 2023, https://www.vie-publique.fr/eclairage/289281-donnees-numeriques-de-sante-quels-enjeux-pour-quel-progres-medical

[9] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JORF n°0022 du 27 janvier 2016

[10] 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)

[11] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JORF n°0141 du 21 juin 2018

[12] Loi n° 94-654 du 29 juillet 1994 relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal ; Loi n° 2004-800 du 6 août 2004 relative à la bioéthique ; Loi n° 2011-814 du 7 juillet 2011 relative à la bioéthique, JORF n°0157 du 8 juillet 2011

[13] Loi n° 2013-715 du 6 août 2013 tendant à modifier la loi n° 2011-814 du 7 juillet 2011 relative à la bioéthique en autorisant sous certaines conditions la recherche sur l'embryon et les cellules souches embryonnaires, JORF n°0182 du 7 août 2013 ; Article L.2151-5 et suivants du code de santé publique

[14] CNIL.fr/quelles-formalites-pour-les-traitements-de-donnees-de-sante-a-caractere-personnel

[15] Conseil d'État, 10ème - 9ème chambres réunies, 19/06/2020, 430810, Publié au recueil Lebon

[16] Conseil d'État, 10ème - 9ème chambres réunies, 19/06/2020, 430810, Publié au recueil Lebon ; Conseil d'État, 10ème - 9ème chambres réunies, 19/06/2020, 434671 & 434684

[17] https://www.cnil.fr/fr/recherches-sante-quelles-formalites ; https://www.cnil.fr/fr/recherche-scientifique-hors-sante-quelle-base-legale-pour-un-traitement-de-recherche

[18] CNIL, Rapport d'activité, 2018

[19] OMS, Rapport sur la santé en Europe, 2021

[20] https://www.justice.gov/criminal/cloud-act-resources

[21] Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations, March 3, 2023 ; Joint US-EU Statement on Electronic Evidence Sharing Negotiations, September 26, 2019

[22] Jean-François Mattei, « Il faut créer une agence de sûreté des algorithmes », Interview dans Alternatives Santé, juin 2020, n° 80.

[23] ESN en France, « Le Cloud Act : une menace pour la souveraineté européenne », https://esnenfrance.com/cloud-act/

[24] Gauthier-Maxence, Céline. "Défis juridiques du droit de la santé à l'ère du numérique et de l'IA." (2024).

[25] CNOM, Livre blanc, p. 60, recommandation 27.

[26] Rapport de l'OMS, op. cit.

[27] N. Le Bouard, « Enjeux juridiques et éthiques de la télémédecine : responsabilités des professionnels et patients. », *Village de la Justice.fr*, 23 mars 2023.

[28] Communication from the Commission to the European parliament, The Council, the European economic and social committee and the Committee of the regions, A European strategy for data, Document 52020DC0066, COM/2020/66 final

[29] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_fr

[30] Ibid

[31] « Espace européen des données de santé : protéger la santé des citoyens de l'UE à l'ère du numérique », 16/05/2022, https://ec.europa.eu/newsroom/sante/items/745450/fr

[32] Représentation au Luxembourg, « Union européenne de la santé : Un espace européen des données de santé pour les personnes et pour la science », site de la Commission européenne, 3 mai 2022
[33] Regulation (EU) 2022/2554 of the European parliament and of the Council of 14 December 2022, on digital operational resilience for the financial sector and amending Regulations (EC), No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
[34] https://artificialintelligenceact.eu/fr/
[35] Gauthier-Maxence, Céline. "European Cybersecurity and AI Framework: Towards Proactive Regulation for a Secure Digital Future." *EU Law Live* 212 (2024): 1-8.