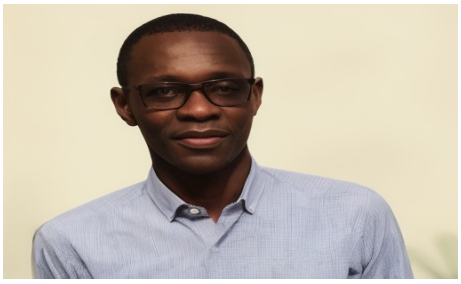

BABA FALL BADIANE

JURISTE EN NUMERIQUE/DPO- SCP LEGALIX

baba.fallbadiane@gmail.com

77 774 50 45

Sujet : l'Encadrement juridique de la gestion électronique des données de santé

Sommaire

Méthodologie et plan de l'étude

L'étude de l'Encadrement juridique de la gestion électronique des données de santé intervient dans le contexte où le Sénégal vise à informatiser le secteur de santé pour l'amélioration de la prestation de services de soins, de la circulation des informations par voie électronique, de la gestion efficiente du système de santé et de la protection des données de santé conformément au plan stratégique santé digitale 2018-2023.

L'encadrement juridique de la gestion électronique des données de santé doit nécessairement promouvoir une politique et des pratiques efficaces en matière de collète et traitement des données des citoyens, de l'administration publique et du secteur privé d'une part et d'autre part, tenir compte de l'impact de la télémédecine, le big data, les objets connectés… de tous les droits numériques tels que la vie privée et les données personnelles.

À cela s'ajoute une croissance exponentielle d'acteurs non régulés comme les GAFAM qui s'intéressent de plus les données de santé ou moins régulé comme les hébergeurs des données de santé et la divulgation, l'utilisation détournée, la manipulation par des personnes non habilitées, le risque de piratage informatique et l'utilisation des données à des fins commerciales, etc.

L'ensemble de ces facteurs incitent les autorités du secteur du numérique à s'interroger : Quel encadrement juridique faudrait-il adopter pour garantir davantage la protection des droits et libertés des individus dans la gestion électronique des données de santé devenues indispensables dans l'évolution actuelle de la société ?

La méthodologie qui a été adoptée pour cette étude comprend essentiellement la recherche documentaire, de données disponibles auprès des bibliothèques en ligne.

Ce travail scientifique est le résultat d'une étude sur « *l'Encadrement juridique de la gestion électronique des données de santé au Sénégal* » afin de mieux régulé les données de santé.

En outre, une étude sur l'Encadrement juridique de la gestion électronique des données de santé nécessite une note introductive des TIC dans le secteur de la santé et une bonne compréhension des concepts qui ne sont pas souvent familiers aux lecteurs (I). C'est dans cette suite logique que des

éléments de réponse mériteraient d'être apportés à la problématique de l'encadrement juridique de la gestion électronique des données de santé.

L'Etat, acteur principal de la protection des données de santé intervient pour encadrer la collecte et le traitement des données de santé dans un cadre normatif (II) et institutionnel (III). Des risques potentiels peuvent résulter des programmes de collecte et de traitement des données de santé (IV). Pour une protection efficace de la gestion électronique des données de santé nous proposons de recommandations à l'endroit des parties prenantes concernées (administration, secteur privé) (V).

I. Note introductive des TIC dans le secteur de santé

Les Technologies de l'Information et de la Communication (TIC) se développent rapidement et sont de plus en plus intégrées dans le quotidien des sénégalais. En effet, le Gouvernement du Sénégal développe activement l'usage généralisé des TIC dans la vie quotidienne au Sénégal à travers ses différentes initiatives nationales telles que décrites dans sa stratégie *« Sénégal Numérique 2025* »[1], adossée au référentiel de développement du Plan Sénégal Emergent (PSE), adopté en 2012[2]. Cela ajoute le plan stratégique santé de digitale 2018-2023. Ces initiatives entraînent une digitalisation du secteur de santé.

L'utilisation des TIC en faveur de la santé, dénommée « *Santé Digitale* », vise l'amélioration de la prestation de services de soins, de la circulation des informations par voie électronique et de la gestion efficiente du système de santé. Le développement de la santé digitale représente une opportunité extraordinaire pour le Sénégal.

La santé digitale est un instrument puissant pour permettre à tous un meilleur accès à la santé et ainsi contribuer à l'atteinte des objectifs de développement durable des Nations Unies[3]. L'utilisation des TIC assurera une meilleure équité dans l'accès aux soins de santé (télémédecine pour un accès électronique aux soins, m-Santé[4]pour notamment améliorer la prévention et la promotion de la santé). Les solutions

[1]Le Sénégal a lancé en 2016 sa stratégie « Sénégal numérique 2025 ».

[2] PSE vise à stimuler une croissance économique soutenue et inclusive et à faire du Sénégal une économie émergente d'ici 2035.

[3] Les objectifs de développement durable sont un appel à l'action de tous les pays pauvres, riches et à revenu intermédiaire afin de promouvoir la prospérité tout en protégeant la planète. Ils reconnaissent que mettre fin à la pauvreté doit aller de pair avec des stratégies qui développent la croissance économique et répondent à une série de besoin sociaux notamment l'éducation, la sante, la protection sociale et les possibilités d'emploi, tout en luttant contre le changement climatique et la protection de l'environnement. Source : https : //www.un.org.

[4] La m-Santé (santé mobile) englobe les pratiques médicales et de santé publique supportées par les objets connectés et appareils mobiles, tels que les téléphones mobiles, les PDA (assistants numériques personnels), les

de santé digitale réduiront les distances en permettant de connecter les patients et les structures de santé aux spécialistes. Enfin, la santé digitale contribue à remettre le citoyen et le patient au centre de l'acte médical. Le numérique doit faciliter la mise en œuvre de la stratégie de la carte sanitaire mais de manière plus large, renforcer l'accès à la santé à plusieurs niveaux : l'offre de soins, la traçabilité du patient, la formation continue du personnel de santé, la promotion de la santé, la prise en charge et la prévention des maladies, la gouvernance sanitaire à travers la collecte de données sanitaires en temps réel, la dématérialisation du parcours du patient, et la responsabilisation des patients par un accès accru à l'information de santé.

Toutes ces informations montrent que le Sénégal est bien dans la dynamique d'utiliser les technologies au service de la santé. Et cette dernière est considérée comme le domaine qui regorge de données personnelles qui sont en fait des données sensibles. En effet, qui parle de technologie, dit traitement automatisé des données personnelles. L'utilisation des technologies dans le domaine de la santé traite avec une quantité considérable des données personnelles des patients, classées sensible. C'est dans ce cadre que Maître Frédéric Forster, Avocat à la Cour d'appel de Paris, affirme que : « *C'est cette collecte massive de données à caractère personnel qui est souvent présentée comme étant la contrepartie de la gratuité des services sur internet, le « produit » étant la personne qui communique ses données aux différents acteurs de l'internet* »[5].

En effet, l'informatisation dans le secteur de santé implique pour tous les utilisateurs la fourniture d'informations sensibles, condition sine qua none pour accéder aux technologies, telles qu'Internet, la téléphonie mobile[6] et autres objets connectés. C'est à juste raison que le professeur Abdoulaye SAKHO soutient *« qu'il n'y a pas de secteur du numérique, c'est la forme d'expression de l'économie contemporaine. Tout devient numérique dans la société actuelle, il est dans le transport, l'énergie, les banques »*[7].

Ainsi, compte tenu de l'importance des données de santé, comme l'élément principal exploité à l'ère du numérique, la collecte et le traitement constituent des enjeux majeurs pour l'Etat du Sénégal en raison de la multitude d'intervenants dans la circulation et l'utilisation des informations personnelles sur les réseaux : GAFAM, les grandes entreprises internationales, les professionnels de santé et les hôpitaux.

Smartphones, et autres appareils sans fil. La m-Santé comprend aussi les applications pour mobiles aux objets connectés (bracelets, capteurs de paramètres physiologiques, glucomètres connectés etc.)

[5] P. F. DRAME et R. SARR, L'impact du règlement sur la protection des données (RGPD) en Afrique, Harmattan, 2021, P. 15.

[6] M. LO, La protection des données à caractère personnel en Afrique, Baol Editions, 2017, P. 19

[7] SAKHO (A), « article publié Sud Quotidien » : « « Le numérique n'est pas un secteur d'activité, mais une forme d'expression de l'économie », le 7 juin 2017, disponible sur le : https://www.osiris.sn/Abdoulaye-SakhoProfesseur-agrege.html.

Protéger ces données à revient à protéger l'intimité, la dignité et les autres droits fondamentaux des patients comme le droit à la vie privée, le droit à l'image, le droit à l'honneur, etc.

La gestion électronique de documents, connue, généralement sous l'acronyme GED ou EMD pour "*electronic document management*" en anglais, désigne un procédé informatisé visant à organiser et gérer des informations et des documents électroniques au sein d'une organisation ou encore des logiciels permettant la gestion de ces contenus documentaires.

Mais, pris dans ce sens, cette expression ne prend pas totalement en compte toutes les actions que recouvre la gestion électronique telle que nous voulons l'employer dans le cadre de cette étude.

Le substantif « *gestion* », synonyme du « *maniement* » selon le dictionnaire Robert, renvoie dans le langage informatique au contrôle du fonctionnement d'une entité notamment des informations ou des périphériques. Le maniement d'informations consiste dans leur collecte, leur manipulation, leur conservation et leur échange. L'adjectif « *électronique* » associé ramène à une gestion par support informatique. En effet, en l'absence de définition du terme « électronique » dans la législation sénégalaise, celle donnée par la loi uniforme canadienne peut nous éclairer. « *Électronique* », qualifie ce qui est « *créé, transmis ou mis en mémoire sous forme numérique ou sous une autre forme intangible par des moyens électroniques, magnétiques ou optiques ou par d'autres moyens capables de créer, d'enregistrer, de transmettre ou de mettre en mémoire de façon similaire à ceux-ci* [8] ». Ainsi présentée, l'expression « *gestion électronique* » se rapproche de ce que la législation sénégalaise dénomme « *traitement automatisé* ». Et c'est dans ce sens que cette expression doit être comprise dans le contexte de cette analyse.

Aux termes de l'article de 2c de la convention du Conseil de l'Europe du 28 janvier 1981 dite convention 108, un « *"traitement automatisé" s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement de données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, installation ou diffusion* ».

La loi de 2008 ne définit pas le traitement automatisé des données mais le traitement des données en y incluant les procédés automatisés. On entend par traitement de données à caractère personnel : « *toute opération ou ensemble d'opérations prévues à l'article 2 de la présente loi effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou*

[8] Article 1 de la loi uniforme canadienne sur le commerce électronique.

toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel » . Cette définition proposée par la loi de 2008, couvre un large choix de procédés utilisés pour le traitement ou la gestion des données. Le support du traitement peut donc être papier, électronique, optique ou autre. Dans le cadre de cette étude, la gestion est électronique ; le procédé utilisé entre donc dans le champ d'application de cette définition.

La gestion électronique des données crée un lien juridique entre le responsable de traitement, le destinataire et la personne concernée. Subsidiairement, le lien peut être quadripartite avec l'intervention d'un hébergeur. « *Le responsable de traitement* », « *le destinataire* » et « *la personne concernée* » sont définis par la législation Sénégalaise.

Quant à l'expression « *données de santé* » est définie par l'article 1 de la convention de Malabo comme « *toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques précitées* ». Quant à l'expression des « *données génétiques* » elle se réfère *« toute donnée concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés* [9]».

Cette définition comprend donc :

Les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services :

- Un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ;
- Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques ;
- Les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée (indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro)[10].

Les données de santé sont considérées comme des « *données à caractère personnel* » caractérisées par une certaine sensibilité qui justifie les mesures particulières prises pour assurer leur sécurité.

[9] Article 4 de la Loi n° 2008 – 12 sur la Protection des données à caractère personnel
[10] Qu'est-ce ce qu'une donnée de santé ? | CNIL

Aux termes de l'article 4 de la loi de 2008, constitue *« une donnée à caractère personnel toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ».*

Une donnée de santé est donc une donnée relative à sa santé pouvant permettre d'identifier un individu. Elle fait partie de celles qui sont régies par la section de la loi de 2008 relative aux dispositions propres à certaines catégories de données[11]. Ce sont des données que la loi a qualifié de *« données sensibles*[12] ». Elles bénéficient d'une protection renforcée par le droit positif. Ces données sont dites sensibles car leurs traitements comportent des risques beaucoup plus considérables que ceux des autres données à caractère personnel dans la mesure où cela engage d'autres droits fondamentaux notamment la liberté d'opinion, la liberté de conscience, ou peut occasionner d'éventuelles discriminations. Ainsi, les données de santé sont-elles préservées pour protéger l'individu contre toute discrimination due à son état de santé. Tous les textes précités s'accordent sur le fait que ces données, par nature, particulièrement sensibles et vulnérables du point de vue des droits fondamentaux et de la vie privée méritent une protection spécifique ; c'est pourquoi elles ne devraient pas faire l'objet d'un traitement, à moins que la personne concernée n'y consente expressément ou que la loi ne le permette pour des questions d'intérêt général.

En réalité, la société actuelle multiplie les traitements automatisés de données de santé pour des raisons économiques. Or, en l'état actuel de la législation sénégalaise (et plus encore au niveau international), il existe plusieurs questions non encore élucidées pour garantir la protection des données sensibles.

La donnée est désormais au cœur de l'ensemble des activités, d'où la nécessité de bien gérer ces données, et d'en garantir l'exactitude et l'intégrité. Son encadrement juridique est assuré, à la fois, par le droit commun notamment la constitution, le Code de la Santé, le Code de la déontologie, la loi relative à l'exercice de la médecine et les dispositions du Code pénal relatives au secret médical et des textes spécifiques relative au traitement automatisé de toutes les données des données de santé. Ces données, même si elle constitue une source d'économie, engendre des problèmes de protection de la

[11] Ce sont « *des données à caractère personnel qui font apparaître, directement ou indirectement, l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée* ». Article 40 de la loi de 2008 sur la protection des données à caractère personnel.

[12] Toutes les données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives. Article 4 de la loi de 2008 sur la protection des données à caractère personnel.

vie privée auxquels le gouvernement sénégalais tente de faire face en créant l'un des meilleurs cadres juridiques au monde, en la matière. Mais, de grands chantiers comme celui du dossier médical personnel attendent toujours d'être réalisés et le droit de la santé se voit devancer et entraîner par les progrès technologiques. Le développement de la télésanté bouleverse les relations au sein du colloque singulier entre le soignant et le soigné. L'extension des droits des patients, le partage de responsabilité, l'augmentation du nombre d'intervenants, le secret médical partagé et l'augmentation des risques constituent de nouveaux enjeux avec lesquels il faut, désormais compter. Une autre question cruciale est celle posée par le manque d'harmonisation des législations augmentant les risques en cas de partage transfrontalier de données de santé.

II. Cadre normatif

La protection de la vie privée est un droit fondamental consacré dans tous les textes internationaux et nationaux. En fait, parler de la vie privée, c'est aussi penser aux données personnelles qui sont sans nul doute une sphère privée de la personne. Ces dernières sont de plusieurs type notamment les données classées top secrètes. Il s'agit, parmi lesquelles, des données de santé. Du fait de leur sensibilité, leur traitement est particulièrement encadré par le droit commun (A) et le droit spécial (B).

A. Le droit commun

Le droit positif impose certaines règles aux responsables de traitement automatisé de données personnelles. La plupart d'entre elles sont communes à toutes les données personnelles : c'est le respect de la vie privée du patient, tandis que quelques-unes sont propres aux données de santé : c'est le secret médical.

- **Le respect de la vie privée**

Toutes les autorités nationales et internationales en charge de la régulation des traitements automatisés des données de santé, conscientes que l'informatique a fait de la vie privée un des problèmes majeurs de notre ère, se sont déjà penchés sur la question de la vie privée à travers les textes qu'elles édictent. Le fondement du droit au respect de la vie privée émerge des droits fondamentaux[13] que sont le droit à la vie, le droit à l'inviolabilité de sa personne, le droit de ne pas pouvoir publier certaines informations sur sa vie privée, mais le droit à la liberté et le droit à la propriété. Selon l'article 3 de la déclaration

[13]MICHEL, L. Secret médical et dossier informatisé. Louvin médical n° 120. Belgique 2001. p. S131

également universelle des droits de l'homme, *« tout individu a droit à la vie, à la liberté et à la sûreté de sa personne »*.

Le droit à la vie privée est une notion très récente au Sénégal. En effet, jusqu'à présent, la question du droit à la vie privée ne se pose pas : chaque personne est sous l'œil permanent de la communauté, qui a un droit de regard, au propre comme au figuré, sur elle. Les conduites individuelles sont ainsi disciplinées par cette surveillance de tous, par tous, sur tous. Les dérives aux normes collectives pouvaient être punies sans que la question du droit ne soit pas posée.

En l'absence de définition légale, on pourrait se référer à la jurisprudence, qui n'en a pas donné non plus mais est constante en la matière. Elle a entrepris d'en déterminer le contenu. La vie privée inclut l'état de santé[14], la vie sentimentale, l'image[15], la pratique religieuse, les relations familiales et, plus généralement, tout ce qui relève du comportement intime[16] d'un individu. La doctrine qui n'en dit pas autre chose est abondante sur le sujet[17]. RIVERO, fut l'un des auteurs les plus inspirés par la problématique de la vie privée. Pour lui, « *le droit, de longue date, reconnaît à l'individu une certaine sphère d'activité dont il est libre de refuser l'accès à autrui : c'est sa vie privée. À cette idée se rattachent, traditionnellement, la protection du domicile, qui est, par excellence, le siège de la vie privée, le secret de la correspondance et des conversations téléphoniques, le secret professionnel imposé à ceux que leurs fonctions appellent à pénétrer dans la vie privée des autres* »[18]. La vie privée est donc une notion subjective dans la mesure où même si elle est "la chose là mieux partagée, chaque individu peut en avoir une conception propre justifiée par différents facteurs, notamment sa culture. Cela peut expliquer la diversité de ses acceptions au niveau de la doctrine et la difficulté des législateurs à donner une définition.

[14] CEDH 10 octobre 2006, L.L. c. France, [en ligne], n° 7508/02. Disponible sur : Consulté le 1 juin 2014.
[15] Cour de cassation, 1ère chambre civile, 12 juillet 2001, n° 98-21.337. Dalloz, n° 17, 25 avril 2002, p. 1380- 1383 BIGOT, Christophe (droit à l'image), Cass. civ. 1ère, 24 Septembre 2009. Société Jacky Boy Music c. M Salvador. n° 08-11.112. Bull 2009, n° 184, p. 166. JurisData: 2009-049655.
[16] 6Cour de Cassation Chambre civile 1, 7 février 2006, N° de pourvoi : 04-10941. http://www.legifrance.gouv.fr/affichJuriJudi.do ? idTexte=JURITEXT000007051655.
[17] « Pour M. RAVANAS, " la vie privée est pour l'individu une sphère secrète de la vie où il a le pouvoir d'écarter les tiers ". Ce pouvoir est considéré par le consentement donné ou refusé par l'individu concerné. La vie privée était également définie par Platon comme la part de l'être humain inaccessible à autrui sans le consentement de l'intéressé. Cette idée sera reprise par le doyen CARBONNIER selon lesquels elle représente " une sphère secrète de vie d'où il « l'individu) a le pouvoir d'écarter les tiers". De son côté, l'Américain NIZER professait que le right of privacy était le droit de l'individu à une vie retirée et anonyme (1939). Enfin J. RIVERO donnera sa définition de la vie privée en la classant dans cette "sphère de chaque existence dans laquelle nul ne puisse s'immiscer sans y être convié". Cette conception, reprise par les différents auteurs cités, vise à préserver le secret la tranquillité de la personne. Cette dernière dispose alors librement de la maîtrise du secret qu'elle peut révéler à sa guise.
[18] RIVERO, Jean. Les Libertés publiques, 1991, p 33.

Son importance est telle que les nations Unies l'ont élevée au rang de la loi fondamentale en adoptant la résolution 68/167, qui appelle tous les pays à respecter et à protéger le droit privée à l'ère numérique.

Le Sénégal a adhéré à tous les instruments internationaux y faisant référence : la déclaration universelle des droits de l'homme (article 12)[19] et le Pacte international relatif aux droits civils et politiques (article 17)[20].

Sur la plan régional, le Sénégal a ratifié en 2016, la Convention de l'Union Africaine sur la cyber sécurité et la protection des données personnelles dont l'un des principaux objectifs, est de mettre en place, dans chaque État partie, un dispositif permettant de lutter contre les atteintes à la vie privée.

Au niveau national, même si l'expression « *vie privée* » n'est pas expressément mentionnée dans la Constitution du Sénégal, le droit au respect de la vie privée à l'ère numérique a un fondement constitutionnel. En effet, l'article 13 de la constitution consacre l'inviolabilité du secret des correspondances électroniques, sauf application de la loi.

Ce cadre légal de protection de la vie privée est renforcé par des dispositions de la loi n° 2016-29 du 08 novembre 2016 portant Code pénal qui sanctionnent les atteintes au droit à la vie privée.

L'article 363 bis du Code pénal, puni d'un emprisonnement d'un an à cinq ans et d'une amende de 500 000 francs à 5.000.000 de francs celui qui au moyen, d'un procédé quelconque, porte volontairement atteinte à l'intimité de la vie privée, tandis que l'article 431-27 réprime la collecte et le traitement des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de la vie privée d'une personne.

Quant à l'article 431-60, il puni d'un emprisonnement de cinq ans à dix ans et d'une amende de 500.000 francs à 10.000.000 de francs ou l'une de ces deux peines celui qui, par un moyen de communication électronique, affiche, expose ou projette aux regards du public, tout contenu contraires aux bonnes mœurs.

- **Secret médical**

[19] Article 12 de la Déclaration Universelle des Droits de l'Homme « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

[20] Article 17 Pacte international relatif aux droits civils et politiques « Chacun a droit à la protection de sa vie privée ».

Le secret médical s'impose à tout médecin. Véritable obligation de discrétion professionnelle, il représente un droit fondamental pour le patient. Le secret médical incarne un des piliers de l'exercice de la médecine, puisque « *il n'y a pas de soins sans confidences, de confidences sans confiance, de confiance sans secret* »[21].

Dans le code de déontologie de l'Ordre national des médecins du Sénégal, il n'est mentionné nulle part une définition du secret médical. C'est l'expression « *secret professionnel* » qui y est plutôt utilisée.

La notion de secret médical couvre l'ensemble des informations que vous portez à la connaissance du professionnel de santé. Cela inclut les informations que vous avez confiées, mais aussi tout ce qui a pu être vu, entendu, compris, voire interprété lors de l'exercice médical. Ainsi sont couverts par le secret professionnel médical : les déclarations d'un malade, les diagnostics, les dossiers, mais aussi les conversations surprises au domicile lors d'une visite, les confidences des familles[22]. Toutes ces informations sont des données de santé.

Toutefois, selon le médecin légiste Amadou Sow[23], le dossier médical est un recueil d'informations du patient. Il s'agit d'informations que le patient lui-même a données, des informations recueillies par le médecin auprès de son entourage, des constatations du médecin chez le patient ainsi que les éléments des examens, des analyses, des radios, etc.

Chaque professionnel qui connaît ou suit l'état de santé doit respecter le secret médical. Exemples : médecin, infirmier, kinésithérapeute, psychologue, assistant social, orthophoniste. Ainsi, un professionnel qui a des informations sur vous ne doit pas les communiquer à d'autres personnes[24].

Ces données de santé sont protégées par le secret médical. Ce dernier est prévu par l'article 7 dans le code de déontologie de l'Ordre national des médecins du Sénégal « *Tout médecin est astreint au secret professionnel (mais) il peut en être délié dans les cas prévus par la loi* ».

Le secret médical est un domaine sensible pour le personnel sanitaire en tant que composante du *Serment d'Hippocrate*. D'ailleurs, le président de la République du Sénégal, Macky Sall avait évoqué la question le 26 novembre 2021, en marge de la pose de la première pierre de la polyclinique de l'Hôpital principal de Dakar. Selon le chef de l'ETAT « « *Le secret médical doit être un sujet de réflexion*

[21]Bernard Hoerni dans son livre Ethique et déontologie médicale, 2e édition Masson, juin 2000.
[22]France ASSOS Santé, Secret médical : respect, partage, dérogation et violation : Le Secret médical - Définition (partagé...), Violation, Dérogation (france-assos-sante.org).
[23] Sénégal-Accès à l'information: les limites bien fixées en milieu médical : Sénégal-Accès à l'information: les limites bien fixées en milieu médical - Une information fiable et indépendante sur... (ouestaf.com).
[24]Secret médical : de quoi s'agit-il ? | Service-Public.fr

au Sénégal. Dans ce pays, les gens ont l'habitude de divulguer les maladies de leurs concitoyens. (J'ai aperçu un tel à l'hôpital, il a la Covid), ce n'est pas normal. Un médecin ne doit pas divulguer la maladie de son patient. Un personnel médical n'a pas le droit de violer le secret médical. Sans oublier, un inconnu qui se permet de dévoiler la maladie d'une tierce personne »[25].

Le secret médical impose aux professionnels de santé de ne pas divulguer les données de santé. La violation du secret médical est réprimée par le code pénal en son article 363 : « *Les médecins, chirurgiens, ainsi que les pharmaciens, les sages-femmes et toutes autres personnes dépositaires, par état ou par profession ou par fonctions temporaires ou permanentes, des secrets qu'on leur confie, qui, hors le cas où la loi les oblige ou les autorise à se porter dénonciateurs, auront révélé ces secrets, seront punis d'un emprisonnement d'un à six mois et d'une amende de 50.000 à 300.000 francs ».*

L'obligation au secret apparaît de prime abord simple, puisqu'il s'agit de la traduction professionnelle de l'obligation générale de discrétion et de respect de la personne d'autrui.

B. Le droit spécial

Cadre juridique particulier du traitement des données de santé est assuré par les textes internationaux et les textes nationaux. Ces textes en principe, interdisent de traiter les données de santé. Mais ce principe est assorti d'exceptions et dans les cas où ces données de santé peuvent être traitées, elles sont soumises à une procédure exorbitante du régime de droit commun des traitements de données personnelles.

- **Le principe d'interdiction du traitement automatisé des données de santé**

Le principe de l'interdiction de traiter les données sensibles, notamment les données médicales, a des sources tant supranationales que nationales.

- **Les sources supranationales du principe de l'interdiction**

S'il est admis que la dangerosité d'un traitement de données pour les droits et libertés de la personne concernée s'apprécie en fonction de la finalité poursuivie par le responsable du traitement, s'agissant des données *« sensibles »*, dont celles de santé, leur seul contenu expose déjà leur titulaire à des risques sans tenir compte de la finalité. Toute utilisation de celles-ci impliquant ainsi automatiquement

[25] Secret médical : « Un médecin ne doit pas divulguer la maladie de son patient » : Secret médical : « Un médecin ne doit pas divulguer la maladie de son patient » (MackySall) (senego.com).

des risques d'atteinte aux droits et aux libertés, les législateurs ont décidés d'en interdire le traitement. Cette interdiction a été posée par la convention n°108 et la convention de Malabo.

La convention n° 108

La convention 108 dispose que : « *les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même des données à caractère personnel concernant des condamnations pénale*s »[26]. Ainsi, la convention est le premier texte international à valeur contraignante à consacrer le principe de l'interdiction de traitement des données de santé en tant que « *catégories particulières de données* ». Cette disposition subordonne le traitement des données sensibles à des garanties appropriées apportées par le droit interne. Cette garantie doit avoir pour objectif de *« prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, les droits et libertés fondamentales de la personne concernée, notamment les risques de discrimination »*[27].

Antérieurement à la Convention, un ensemble de lignes directrices du Conseil de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel du 23 septembre 1980 avait déjà émis des recommandations[28] allant dans ce sens pour l'ensemble des données personnelles. Mais elles fixaient un principe de limitation en matière de collecte des données à caractère personnel sans préciser celles qui sont considérées comme sensibles et ne mentionnaient pas particulièrement les données de santé. L'OCDE laissait toute latitude aux États membres de le faire *« selon les traditions et les attitudes propres à chaque pays membre*[29]» sachant qu'aucune donnée n'est en elle-même privée ou sensible, mais peut le devenir en fonction du contexte et des circonstances dans lesquels elle est traitée. Certes, ce n'était qu'une recommandation, mais elle jetait les prémisses d'une harmonisation en matière de protection des données personnelles à partir des motifs[30] de

[26]Convention 108 du 21 janvier 1981, Article 6 – Catégories particulières de données

[27] Convention 108 du 21 janvier 1981 (version modernisée), Article 6 – Traitement de données sensibles.

[28] Recommandation du Conseil de l'OCDE concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel du 23 septembre 1980, 5ème partie, paragraphe 7, Les points 50 à 52. Disponible sur : http://www.oecd.org/document/57/0,3343,fr_2649_34255_1815225 _1_1_1_1,00.html.

[29] Point 51, paragraphe 7 de la recommandation du 23 septembre 1980 op. cit..

[30] « Compte tenu de l'essor pris par le traitement automatique de l'information, qui permet de transmettre de vastes quantités de données en quelques secondes à travers les frontières nationales et même à travers les continents, il a fallu étudier la question de la protection de la vie privée sous l'angle des données de caractère personnel. Des législations relatives à la protection de la vie privée ont été adoptées ou le seront prochainement dans près de la moitié des pays de l'OCDE (l'Allemagne, l'Autriche, le Canada, le Danemark, les États-Unis, la France, le Luxembourg, la Norvège et la Suède ont promulgué une législation. La Belgique, l'Espagne, les PaysBas et la Suisse ont établi des projets de loi) en vue de prévenir des actes considérés comme constituant des violations des droits fondamentaux de l'homme, tels que le stockage illicite de

l'élaboration de ses lignes directrices. Cela a probablement eu pour effet d'accélérer l'adoption de la Convention n° 108 pratiquement 4 mois plus tard. Depuis 2011, un processus de modernisation de la convention a été lancée en vue d'adapter les dispositions à l'évolution actuelle des technologies de l'information et de la communication. S'agissant des données sensibles, l'article 6 intitulé traitement « *catégories particulières de données* » a été remplacé par le « *traitement de données sensibles* ». La liste des données dites sensibles a été complétée par les données génétiques et biométriques, des données relatives à l'appartenance syndicale et celles concernant les infractions et les autres mesures de sûreté connexes. Alors que l'interdiction de traitement était exprimée par l'expression « *les données (…) ne peuvent être traitées automatiquement à moins que » la proposition de modernisation emploie l'expression « le traitement (…) n'est autorisé qu'à la condition que* ». Si ces différences dans la terminologie ne doivent pas être interprétées comme entraînant des divergences autres que de pure forme, cette formule laisse sous-entendre une plus grande tendance à l'autorisation de traitement ou, du moins, une plus grande tolérance, que la première. Il faut croire que l'intérêt économique du traitement accru de données, particulièrement des données de santé, a influencé les rédacteurs de cette proposition de modernisation. A défaut de passer du principe de l'interdiction à celui de l'autorisation, le ton a été assoupli ; ce qui n'est pas rassurant pour l'avenir de la protection des données sensibles de plus en plus en proie à la commercialisation.

La Convention 108 a été suivie de l'adoption par plusieurs États membres de législations sur la protection des données personnelles.

Convention de Malabo

Toujours dans la logique de défendre le principe de l'interdiction du traitement des données de santé, la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel a pris avec pied ferme de protéger les données de santé. Rappelons que la présente convention portant adoption d'un cadre juridique sur la cybersécurité et la protection des données à caractère personnel prend en charge les actuels des États membres de l'Union Africaine aux plans sous régional, international en vue de l'édification de la Société de l'information.

données de caractère personnel qui sont inexactes, l'utilisation abusive ou la divulgation non autorisée de ces données. » 1 er paragraphe de la préface de la recommandation op. cit

Elle vise à la fois à définir les objectifs et les grandes orientations de la société de l'Information en Afrique et à renforcer les législations actuelles des États membres et des Communautés Économiques Régionales (CER)[31] en matière de technologies de l'Information et de la Communication.

Elle réaffirme l'attachement des États membres aux libertés fondamentales et aux droits de l'homme et des peuples contenus dans les déclarations, les conventions et autres instruments adoptés dans le cadre de l'Union Africaine et de l'Organisation des Nations Unies.

Elle considère aussi que la mise en place d'un cadre normatif sur la cybersécurité et la protection des données à caractère personnel tient compte des exigences de respect des droits des citoyens, garantis en vertu des textes fondamentaux de droit interne et protégés par les conventions et traités internationaux relatifs aux droits de l'Homme, particulièrement la Charte africaine des droits de l'Homme et des peuples.

L'objet de la convention Malabo est présenté par son article 8 comme visant, d'une part, « *la protection des libertés et des droits fondamentaux des personnes physiques, notamment de la vie privée, à l'égard du traitement des données à caractère personnel et, d'autre part, la garantie de la libre circulation des données à caractère personnel entre États membres sans limitation justifiée par l'insuffisance de protection des personnes concernées* ».

Pour ce qui est des traitements portant sur des catégories particulières de données, l'article 14 -1 prévoit que : « *Les États parties s'engagent à interdire la collecte et tout traitement qui révèlent de l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée* ». Cette disposition de la convention illustre bien la volonté de cette dernière de participer à la protection des données personnelles de manière générale et des données de santé en particulier. Juste qu'ici, on constate que les dispositions juridiques en la matière ont toutes données une protection renforcée sur le fondement du caractère sensible des données de santé. Ces dernières sont, selon les textes évoqués tout au long de notre argumentaire, échappées à tout traitement, quelle que soit sa nature et sa forme.

- **Les sources nationales**

Le respect de la vie privée a été consacré par tous les principaux textes internationaux, mais leur proclamation de ce principe qui suppose une non-ingérence, une abstention de l'État ou de toute autre

[31]CER, pilier de la communauté économique africaine crée en 1991 par le Traite d'Abuja dans le but de fournir au continent un cadre général pour son intégration économique.

personne n'est pas suffisante pour protéger l'individu face au développement de l'informatique. C'est le sens de la loi n°2008-12 du 25 janvier 2008 du Sénégal portant sur la protection des données à caractère personnel. Ce texte reste la base du système sénégalais en matière de traitement des données personnelles.

Le législateur sénégalais a fait une catégorisation des données personnelles en tenant compte de leur nature. De ce fait, il existe des données sensibles dont la loi a pris des mesures strictes pour bien les protéger. C'est pour cela que leur traitement est assorti d'une interdiction selon l'article 40 de la loi de 2008 : en ces termes, « *il est interdit de procéder à la collecte et à tout traitement qui relèvent de l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétique ou généralement celles relatives à l'état de santé de la personne concernée* ». Le fondement de cette interdiction réside dans la volonté du législateur de consacrer dorénavant plus d'attention à la protection de la vie privée.

La loi de 2008 est soutenue dans la répression du traitement illégal des données de santé par le code pénal. En effet, l'article 431 - 21 du code pénal dispose que : « *Celui qui hors les cas prévus par la loi, met ou conserve sur support ou en mémoire informatique sans le consentement exprès de l'intéressé, des données (...) qui sont relatives à la santé (...), est puni d'un emprisonnement d'un à sept ans et d'une amende de 500 000 CFA à 10 000 000 ou de l'une de ces peines* ». Le code pénal a également tenu compte de l'extension précitée en incluant les traitements non informatisés dans le champ d'application des dispositions de l'article 431 - 21 du code pénal.

Comme on le constate, beaucoup de dispositions ont été prises tant au plan international que par la législation Sénégalaise pour prohiber le traitement des données sensibles et surtout celles relatives à la santé. Mais, les législateurs restent objectifs, car ils n'ignorent pas que leur traitement peut s'avérer nécessaire dans l'évolution de la société. C'est ce qui justifie que des exceptions soient admises au principe.

- **Les exceptions au principe**

Conformément aux dispositions internationales et communautaire, le droit sénégalais interdit en principe le traitement des données de santé, en tant que catégorie particulière de données à caractère personnel[32], mais prévoit des dérogations énumérer par l'article 43 :

- ✓ Lorsque la personne concernée a donné son consentement ;

[32] V. l'article 40 de la loi n°2008-12 du 25 janvier 2008 du Sénégal.

- ✓ Lorsqu'il porte sur des données manifestement rendues publiques par la personne concernée ;
- ✓ Lorsqu'il est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où celle-ci se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- ✓ Lorsqu'il est nécessaire à la réalisation d'une finalité fixée par ou en vertu de la loi ;
- ✓ Lorsqu'il est nécessaire à la promotion et à la protection de la santé publique y compris le dépistage ;
- ✓ Lorsqu'il est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée ;
- ✓ Lorsqu'il est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- ✓ Lorsqu'il est nécessaire aux fins de médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit de son parent ou lorsque les services de santé agissent dans l'intérêt de la personne concernée. Les données sont traitées sous la surveillance d'un professionnel des soins de santé qui est soumis au secret professionnel.

- **Le traitement des données santé : un régime exorbitant**

Principes de base

Tout traitement de données de santé obéit à un certain nombre de principes qui doivent être respectés par tout responsable de traitement de ces dites données. En effet, ces données recueillies font partis de la vie privée de la personne d'où l'intérêt de les mettre en état de toute atteinte. Parmi ces principes, on peut citer :

Le principe d'exactitude[33] ; l'exactitude des données collectées est un gage de la qualité du traitement. C'est pourquoi les législations ont pris le soin de veiller à ce que les responsables de traitement vérifient l'exactitude et la pertinence des données collectées et qu'elles demeurent intègre. Les données collectées doivent donc être exactes et, si nécessaire, mise à jour périodiquement[34] ou lors de leur utilisation.

[33] V. loi n°2008-12 du 25 janvier 2008 du Sénégal, art 36 ; V. aussi la convention africaine sur le cyber sécurité et la protection des données à caractère personnel, art 13, Principe 4.
[34] V. Délibération n° 2014-24/CDP du 20 juin 2014 relative à un système de pointage biométrique des Cours Sainte marie de Han.

Le principe de finalité[35] ; celui-ci veille à la protection des individus qui repose essentiellement sur le respect de la finalité du traitement déclare auprès de l'autorité de régulation. Ce principe suppose que les informations recueillies ne puissent être collectées et traitées que pour une finalité déterminée.

A cote de ce principe, il y a celui dit principe de proportionnalité[36] qui exige la collecte des données strictement nécessaire à la finalité poursuivie. C'est pourquoi les législateurs prévoient que les données doivent être adéquates, pertinentes et non excessive au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement. Ce contrôle de proportionnalité repose sur l'existence d'un texte législatif ou règlementaire. A défaut, il appartient à l'autorité de protection d'effectuer une analyse in concreto[37] au regard des éléments des dossiers.

En dehors de ces principes sus évoqués, existe d'autres comme le principe de légitimité[38] qui se définit comme tout traitement portant sur les données à caractère personnel doit obligatoirement avoir une base juridique, c'est-à-dire, une légitimité. Ce principe, consacré par l'article 12 de la Déclaration Universelle des Droits de l'Homme interdit « l'immixtion arbitraire »[39] de l'Etat ou des entreprises dans la sphère de la vie privée. A cet effet, pour qu'un traitement soit légitime, la personne concernée doit donner son consentement de manière expresse. Le consentement donné doit être non vicié et spécifique au traitement en question.

A cote de ce principe, il y a également le principe de licéité[40]. Ce principe voudrait que tout traitement de données personnelles soit loyal et licite. Le traitement loyal suppose une totale transparence du traitement, en particulier vis-à-vis des personnes concernées et de l'autorité de protection. A cet effet, les traitements doivent être expliqués aux personnes concernées de façon claire et précise. La licéité quant à elle, suppose que le traitement soit conforme à une disposition législative ou règlementaire. Tel est le cas, lorsqu'il y a collecte de données sensibles dont le traitement est encadré par des textes de

[35] V. loi n°2008-12 du 25 janvier 2008 du Sénégal, art 35 ; V. également l'acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO, art 25 ; V. dans la même logique sur ce principe la convention africaine sur le cyber sécurité et la protection des données à caractère personnel, art 13, Principe 3.
[36] V. loi n°2008-12 du 25 janvier 2008 du Sénégal, art 35 alinéa 2 ; V. également l'acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO, art 25 alinéa 3.
[37] Mot latin traduisant que l'autorité de protection doit procéder à une analyse concrète des choses afin de pouvoir s'assurer du respect de la loi par le responsable de traitement
[38] V. loi n°2008-12 du 25 janvier 2008 du Sénégal, art 33 ; V. également l'acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO, art 23 ; DECRET n° 2008-721 du 30 juin 2008 portant application de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel, art 32.
[39] 1 Cette Déclaration a pris la ferme décision à travers son considérant 12 que la sphère prive de la personne ne doit pas faire l'objet d'atteinte sans aucune justification DECRET n° 2008-721 du 30 juin 2008 portant application de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel
[40] V lois n°2008-12 du 25 janvier 2008 du Sénégal, art 34 ; V. la convention africaine sur le cyber sécurité et la protection des données à caractère personnel, art 13, Principe 2 ; V. l'acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO, art 24 ;

lois. Ces principes ouvrent des exceptions lorsqu'il s'agit d'un traitement nécessaire à la défense des intérêts vitaux d'une personne. Dans ce cas, c'est la loi qui autorise une telle dérogation parce qu'il y a une nécessité qui se pose. Raison pour laquelle la loi fait légitimer le traitement des données personnelles de santé dans la mesure où il y a une nécessite pour la personne qui impose un tel traitement. Le traitement de ces types de données est autorisé par la loi lorsque la personne en question se trouve dans l'incapacité physique[41] ou juridique de faire valoir ses droits. Dans ces cas précis, la loi fait une dérogation au principe d'interdiction du traitement des données de santé.

Les droits des personnes concernées

Les personnes concernées sont celles dont les données sont collectées. La loi prévoit un certain nombre de droits que les personnes doivent pouvoir exercer. Et c'est au responsable de traitement d'assurer l'effectivité de ces droits. Il faut rappeler que les dispositions générales de la loi de 2008 sur la protection des données à caractère personnel relatives aux droits des personnes et aux obligations de responsable du traitement sont celles applicables aux données de santé.

Il faut rappeler que les dispositions générales de la loi de 2008 sur la protection des données à caractère personnel relatives aux droits des personnes sont celles applicables aux données de santé.

Les droits reconnus aux personnes des données de santé sont.

- Le droit à l'information (article 58) ;
- Le droit d'accès (article 62) ;
- Le droit d'opposition (article 68)
- Le droit de rectification et de suppression (article 69).

Les obligations

Comme pour tous les traitements relatifs aux données personnelles, les responsables du traitement de données de santé doivent, prioritairement, veiller à la sécurité et à la confidentialité des informations conformément à la loi de 2008. Mais, compte tenu de la sensibilité de ces informations, le droit positif se montre plus rigoureux à leur égard. Le non-respect de cette obligation les expose à des sanctions pénales.

L'article 71 de la loi de 2008 dispose que « *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées,*

[41] La personne en question se trouve dans des situations où elle ne peut pas donner son consentement.

ou que des tiers non autorisés y aient accès ». C'est à dire que les responsables de traitements de données doivent mettre en œuvre toutes les mesures techniques et toute l'organisation appropriées pour assurer la protection des données. Ces mesures doivent viser à prévenir la destruction accidentelle ou illicite, la perte accidentelle, la mise à jour, l'altération, la diffusion ou l'accès non autorisé aux données. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger[42]. C'est pourquoi, Il est nécessaire de définir précisément les personnes ou catégories de personnes autorisées à enregistrer, modifier ou traiter les données et, pour les traitements les plus sensibles, de prévoir des mesures de sécurité appropriées.

L'obligation de sécurité pèse principalement sur le responsable du traitement, même lorsqu'il a recours aux services d'un hébergeur. La responsabilité par rapport à la sécurité ne peut jamais être impartie entièrement à un tiers. Une impartition de services équivaut à l'impartition de sa réputation, de la protection de ses données, des risques associés à cette activité et à sa conformité réglementaire. Le fournisseur de services a la responsabilité de rendre les services de façon sécuritaire, par contre toute divulgation ou bris de sécurité demeurera, à l'égard des tiers, la responsabilité du client[43].

Dans un souci de sécurité les informations ne peuvent être conservées de façon indéfinie[44] dans les fichiers informatiques. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier. En effet, plus on détient de données, plus le risque de détournement est grand.

Ce principe est d'importance capitale, car il conditionne la fiabilité du traitement. C'est un gage de confiance à l'égard des titulaires des données à traiter. En matière de santé, par exemple, le secret professionnel dont est tenu le médecin par le Code de déontologie étend le secret professionnel à tout ce que le médecin a vu, connu, appris, constaté, découvert ou surpris dans l'exercice de sa profession[45]. Cette confidentialité apparaît comme un outil qui permet la préservation de valeurs : permettre l'accès aux soins de santé sans crainte de divulgation.

Tous les principes précités trouvent aussi leur source dans les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel adoptée le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990. Ces principes constituent des orientations que donnent les Nations Unies quant aux règlements

[42] Article 17- 1°, 2éme alinéa, de la directive du 25 Octobre 1995 consacrée à la sécurité des traitements.
[43] PAUL, Daniel. Le droit des technologies de l'information au Québec. P. 166.
[44]Article 72 de la loi de 2008 : Obligation de conservation « Les données à caractère personnel ne peuvent être conservées au-delà de la durée nécessaire qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ».
[45] Article 7 décret n° 67 –147 du 10 février 1967 statuant le code de déontologie médicale.

concernant les fichiers informatisés contenant des données à caractère personnel. Les modalités d'application sont laissées à la libre initiative des États. Comme pour confirmer qu'il n'y a jamais trop de dispositions prises pour assurer la Sécurité de la vie privée, le législateur Sénégalais a complété les obligations des responsables du traitement par des droits reconnus aux titulaires des données à traiter.

III. Cadre institutionnel

Assurer la gouvernance des données de santé revient à sécuriser les informations et faire respecter les règles de protection des données. Ce respect ne peut se faire que par l'institution d'un ou de plusieurs organismes chargés de contrôler le respect des dispositions législatives et règlementaires en la matière

A. **Cellule de la Carte Sanitaire et sociale, de la Santé Digitale et de l'Observatoire de la Santé (CSSDOS**)

La CSSDOS, créée par arrêté n° 8299 du 16 mai 2017, est chargée des missions de l'Innovation et de l'Equité notamment[46] :

- Actualiser, suivre et évaluer la Carte sanitaire et sociale, et la Santé digitale ;
- Organiser la Santé digitale, développer des programmes de Santé digitale (Télémédecine, m-Santé, e-Learning, Dossier Patient Informatisé, harmonisation de l'utilisation des services et applications)
- Assurer le secrétariat exécutif de l'Observatoire de la santé.

La Coordination est chargée :

- Initier, impulser et coordonner les activités de la CSSDOS ;
- Préparer les rencontres des comités de pilotage et des groupes de travail ;
- Préparer et exécuter le budget de la CSSDOS en qualité d'administrateur de crédit.

Unité de Développement de la Carte sanitaire et sociale (UDCS) est chargée :

- Veiller au respect et au développement équitable de la carte sanitaire et sociale ;

[46] La CSSDOS - Portail ESANTE - CSSDOS

- Appuyer la planification opérationnelle du secteur de la sante ;
- Elaborer et suivre le programme de développement de la carte sanitaire et sociale (PDCS).

Unité de Géomatique et de Cartographie (UGC) est chargée :

- Appuyer les opérations de cartographie et de géomatique du secteur ;
- Elaborer et mettre à jour le système d'information géographique santé (SIG Santé), la plateforme cartographique web, les cartes de districts sanitaires, de régions et des zones de responsabilité des formations sanitaires et sociales ;
- Organiser le territoire national en territoires sanitaires cohérents et fonctionnels.

Unité de Santé digitale (USD) est chargée :

- Assurer la coordination et le pilotage des plateformes de santé digitale développées par le MSAS ;
- Veiller à la définition et au respect des standards et de l'interopérabilité des plateformes de Santé digitale ;
- Veiller à la cohérence des projets de santé digitale avec les priorités de la politique sanitaire et les standards.

Unité de l'Observatoire de la santé (UOS) est chargée :

- Faciliter le fonctionnement des groupes de travail de l'Observatoire de la santé ;
- Participer à la recherche de l'information stratégique ;
- Assurer la diffusion de l'information stratégique du secteur.

B. Commission de Protection des Données Personnelles (CDP)

Le principe de bonne gouvernance des données personnelles voudrait qu'on ait une institution en charge de la question afin de mieux faire respecter les droits et libertés des personnes. La régulation

des données à caractère personnel a été toujours une question préoccupant toutes les législations[47] des pays ou organisations[48] qui luttent contre toutes atteintes visant à porter un préjudice aux personnes.

En effet, il est incontestablement vrai que la sécurité des informations ne peut être une réalité que si les règles de protection sont strictement respectées. C'est pourquoi il est institué, dans plusieurs textes sur les données à caractère personnel, un organisme qui, en conformité avec le système juridique interne de chaque pays, est chargé de contrôler le respect des dispositions législatives et règlementaires en la matière.

Ainsi, dans le droit de la CEDEAO, l'acte additionnel rend obligatoire la création d'autorité de protection. Aux termes de l'article 14 *« chaque Etat membre met en place une autorité de protection des données à caractère personnel »*. En outre, l'article 11 de la convention africaine exhorte également ses Etats membres à mettre en place une autorité de protection.

En plus, le protocole additionnel[49] à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données affirme être convaincus que des autorités de contrôle exerçant leurs fonctions en toute indépendance sont un élément de la protection effective des personnes à l'égard du traitement des données à caractère personnel. Des lors, l'article premier alinéa 1,2(a et b) et 3 de ce protocole dispose à ses termes « *Chaque Partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des mesures donnant effet, dans son droit interne, aux principes énoncés dans les chapitres II et III de la Convention et dans le présent Protocole. A cet effet, ces autorités disposent notamment de pouvoirs d'investigation et d'intervention, ainsi que de celui d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne donnant effet aux principes visés au paragraphe 1 de l'article 1 du présent Protocole. Chaque autorité de contrôle peut être saisie par toute personne d'une demande relative à la protection de ses droits et libertés fondamentales à l'égard des traitements de données à caractère personnel relevant de sa compétence. Les autorités de contrôle exercent leurs fonctions en toute indépendance* ».

[47] V. la loi n°2008-12 du 25 janvier 2008, art. 5 ; V. art. 11.1. A. énonce que « chaque Etat partie s'engage à mettre en place une autorité chargée de la protection des données à caractère personnel »

[48] V. la 37ème Conférence internationale des commissaires à la protection des données et à la vie privée Amsterdam, le 27 octobre 2015 ; V. aussi 31ème Conférence des commissaires à la protection des données et à a vie privée Madrid 2009.

[49] Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, Strasbourg, 8.XI.2001, Série des traités européens -n° 181. Cette Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ouverte à la signature à Strasbourg, le 28 janvier 1981.

En tenant compte de ces exigences faites par les textes susmentionnés, le Sénégal en tant que pays membre, a créé la Commission de protection des données personnelles (CDP)[50] autorité administrative indépendante, instituée par la loi n° 2008-12 du 25 janvier 2008, est chargée de vérifier la légalité de la collecte et du traitement des données personnelles des sénégalais et de s'assurer que toutes les précautions sont prises pour qu'elles soient sécurisées.

La CDP a pour mission essentielle de protéger la vie privée et les libertés individuelles et publiques. Pour ce faire, cette commission est investie, pour les besoins de sa mission, des pouvoirs de plusieurs types afin de pouvoir, comme le souhaite la loi, de mieux prendre en charge la régulation des données à caractère personnel. Il s'agit tout d'abord des pouvoirs dits réglementaires. Ce pouvoir permet à la commission de prendre des décisions d'ordre règlementaire. Dotant de ce pouvoir, la commission est habilitée d'édicter des règlements en matière de protection des données personnelles. Cette attribution a été prévue par l'article 16 de la loi de 2008 plus précisément dans l'alinéa 7 disposant que : « *elle présente au gouvernement toute suggestion susceptible de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données ».* Ceci laisse à dire que la régulation participe bien à la perfection de la législation et la règlementation à la protection des données à caractère personnel.

Ensuite, la commission a un pouvoir d'instruction lui permettant de procéder, sur place[51], sur convocation[52] ou sur pièces, a des investigations pour vérifier la conformité d'un traitement à la législation. D'ailleurs, ce pouvoir est prévu par tous les textes de loi[53].

Enfin, en sus ces deux pouvoirs, les autorités de la commission a la protection disposent aussi d'un pouvoir de sanction très dissuasive. Ces sanctions peuvent être d'ordre administratif[54]. Outre sa consécration dans les textes nationaux, la base juridique des sanctions administratives est reprise à l'article 20 de l'acte additionnel de 2010 adopté par la CEDEAO. Ce texte dispose que : « *si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adresse, l'autorité de protection peut prononcer à son égard, après procédure contradictoire (…) un retrait provisoire de l'autorisation accordée, un retrait définitif de l'autorité ou une amende pécuniaire* ». Au niveau national, la commission a, à travers les dispositions nationales, dispose un pouvoir d'instruction. A cet effet, l'article 16 évoque au-dessus dispose dans son alinéa 2 que : « *elle peut, par décision particulière,*

[50] V. Chapitre premier. - Dispositions générales. Article premier, alinéa 2, Commission des données personnelles : la dénomination de la Commission de Protection des Données à Caractère Personnel (CDP) prévue par l'article 5 de la loi sur les données à caractère personnel

[51] La réception et l'examen des déclarations et des demandes d'autorisation.

[52] Le pouvoir d'instruction de l'autorité de régulation.

[53] V. la loi n°2008-12 du 25 janvier 2008, art. 16.

[54] V. Délibération n°2014-018/CDP du Sénégal du 30 avril 2014, société AK- société CEGINUS ; - V. Délibération n°2014-019/CDP du Sénégal du 3 avril 2014, EXPRESSO Sénégal SA.

charger un ou plusieurs de ses membres ou des agents de ses services de procéder à des vérifications portant sur tout traitement et, le cas échéant, d'obtenir des copies de tout document ou support d'information utile à sa mission ».

En sus de toutes ces attributions à la commission de protection, il est à souligner l'importance accordée à la protection des données personnelles qui sont liées à la vie privée des personnes. L'autorité de régulation a été investie de tous ces pouvoirs afin de mieux faire respecter la législation en la matière. Cette régulation est fortement encadrée au Sénégal en plus forte raison lorsqu'il s'agit des données sensibles à l'occurrence les données de santé soumises à l'autorisation. Dans le cadre de son rôle de régulateur des données personnelles au Sénégal, la commission est appelée à faire des délibérations et des avis trimestriels comportant des interdictions et des autorisations des traitements portant sur des données personnelles notamment des données de santé.

Dans cette perspective, au cours de ces deux dernières années notamment l'année 2018 et 2019, et conformément à son programme d'activités annuel, la CDP a émis plusieurs appels à la déclaration aux responsables de traitements des secteurs public et privé, examiné plusieurs dossiers de demande d'autorisation, recueilli des plaintes et rendu visite à des acteurs clés dans le mécanisme de protection des informations nominatives au Sénégal. En dehors des exigences légales en matière de protection des données de santé, la commission veille au grain, pour tout traitement portant sur ces types de données, de se conformer à la législation. Ainsi, dans son avis trimestriel N°01-2018, la commission de protection des données personnelles du Sénégal a rejeté la demande de la société NIYEL S.U.A.R.L[55] en raison du traitement des dossiers médicaux des employés par les services des ressources humaines.

La CDP rappelle, a la société, conformément à l'article 43 de la loi n° 2008-12, que le traitement des données relatives à la doit être mis par en œuvre par un professionnel de la santé[56]. Ceci montre l'importance et la nécessite de protection des données de santé que la loi a accordée à cette catégorie de données. Toujours dans sa mission de réguler le secteur, la CDP a eu, dans son avis trimestriel N°02-2019, à se prononcer sur une demande faite par le cabinet d'étude qui aimerait mener une enquête sur les conditions de vie des étudiants. Cette enquête devrait collecter des données de santé de ces derniers. La commission lui a demandé, en vue du nature sensible des dites données d'avoir une autorisation et de veiller à ce que le traitement de ces derniers soit supervisé par un professionnel de santé. La CDP, l'autorité de régulation au Sénégal veille au respect strict des règles de tout traitement sur les données sensibles notamment les données de santé. En effet, dans son rôle de régulateur, la

[55] Http : //www.niyel.net
[56] V. Loi n° 66-69 du 4 juillet 1966 relative à l'exercice de la médecine et à l'Ordre des médecins, art 1.

CDP a, dans son avis n°04-2019, donne des instructions au centre national de transfusion sanguine (CNTS)[57], dans un traitement de données sensibles dont les mesures de sécurité et de collecte sont jugées faibles. Ainsi, par l'application des articles 4-6, 4-8, 35-2, 71 et 40 de la loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, la Commission a requis des explications au CNTS : Sur la pertinence de la collecte de l'information relative à l'appartenance ethnique dans le formulaire à remplir par un donneur de sang sur les mesures prises pour garantir la sécurité et la confidentialité des dossiers médicaux.

Sous la base de ces instructions formulées par la commission, il appartient au dit centre de se conformer aux exigences demandées par ces types de traitement afin que celui-ci soit valable.

C. L'apport du Sénégal numérique SA dans la gouvernance des données de santé

Structure administrative autonome, SENUM SA[58] est le principal levier de la mise en œuvre du projet e-Gouvernement. Elle a pour mission essentielle de mettre en œuvre la politique d'informatisation définie par le Président de la République. A ce titre, elle est chargée de mener et de promouvoir, en coordination avec les différents services de l'Administration, les autres organes de l'Etat et les collectivités locales, tous types d'actions permettant à l'administration de se doter d'un dispositif cohérent de traitement et de diffusion de l'information, répondant aux normes internationales de qualité, de sécurité, de performance et de disponibilité. Elle s'occupe aussi de la mise en œuvre des systèmes d'information et des infrastructures réseaux de l'ETAT.

Il est important de noter que l'expertise et le leadership du SENUM SA sont aussi reconnus au niveau international. SENUM SA bénéficie d'une reconnaissance de structures étatiques et privées dans les pays de la sous-régions, lesquelles effectuent régulièrement des missions de benchmarketing pour s'inspirer de son fonctionnement, son mode de gouvernance ou encore de son expérience en matière d'exécution des projets comme le projet FUDPE et les projets liés à la Cyber sécurité entre autres[59].

Au plan national, SENUM SA a rendu possible la mise en place d'un point d'échange internet au Sénégal en fin 2016, pour asseoir durablement la souveraineté du Sénégal sur ses données[60].

Elle a fait beaucoup de réalisations en matière de gouvernance numérique, notamment par l'intégration et l'adoption des télé-services dans plusieurs secteurs et la mise en place du

[57] Etablissement public de sante doté d'une importante banque de sang. Il organise fréquemment des journées de don de sang et dispose d'un laboratoire d'analyse médicale ainsi que d'un service d'hématologie.
[58] Article premier de la loi n°2021-39 du 13 décembre autorisant la création de la société nationale dénommée « Sénégal Numérique SA (SENUM) ».
[59] https://www.adie.sn/leadership-et-gouvernance.
[60] https://www.adie.sn/leadership-et-gouvernance.

FUDPE, le Fichier Unifié des Données du Personnel de l'Etat. Selon Ousmane THIONGANE[61], FUDPE a pour but de contribuer à la transparence et à l'amélioration de la gestion des finances publiques ainsi qu'au renforcement de la bonne gouvernance, par la maîtrise des données qui impactent régulièrement sur un des plus gros postes de dépenses du budget général de l'Etat, à savoir le poste « *dépenses de personnel* ».

La nouvelle société nationale, Sénégal Numérique SA[62] (SENUM SA) pourra contribuer de manière significative à l'amélioration du secteur du numérique au Sénégal en matière de partages et de déploiement d'infrastructures, d'hébergement, d'innovation technologique, de concert avec les différents acteurs du secteur à l'instar des opérateurs, des fournisseurs d'accès Internet, des créateurs de contenu, des universités, etc. La stratégie Sénégal Numérique ambitionne de faire du pays une locomotive de la sous-région en matière de digitalisation et de bonne gouvernance.

La souveraineté est, pour une nation démocratique, l'expression sans entrave sur son territoire de la volonté collective de ses citoyens. Le peuple se détermine et fait ses choix par lui-même, sans subordination ni dépendance envers une autorité étrangère. Les seules limitations du pouvoir populaire proviennent du droit international et des traités. L'État moderne est l'incarnation de cette autonomie et de cette indépendance.

En plus des institutions susmentionnées, la Direction Générale du Chiffre et de la Sécurité Systèmes d'Information (DCSSI) joue un rôle très important en matière de gouvernance des données. Il ressort du décret portant création et organisation de la Direction Générale du Chiffre et la Sécurité des Systèmes d'Information, Autorité nationale de la cyber sécurité renforce la protection du secret des informations intérieures et extérieures de l'Etat ; propose aux autorités étatiques des orientations stratégiques en matière de sécurité des systèmes d'information, et de cyber sécurité en général, en liaison avec les organismes intéressés, et d'en suivre la mise en œuvre.

IV. Les risques potentiels liés à la collecte et traitement des données de santé

La collecte et le traitement des données de santé ont émergé comme un élément central dans la modernisation des systèmes de santé, apportant des avantages significatifs en termes de diagnostics, de traitements personnalisés et de recherche médicale. Les données de santé comprennent des

[61] Conseiller Spécial à la Présidence de la République du Sénégal et Coordonnateur de la Cellule Digitale de la Présidence.
[62] https://www.sentresor.org/app/uploads/Loi-n%C2%B02021-39-du-13-12-2021-autorisant-cre%CC%81ationSocie%CC%81te%CC%81-Se%CC%81ne%CC%81gal-nume%CC%81rique-SA-SENUM-SA.pdf.

informations essentielles, qui intéressent les administrations de santé nationales et internationales, comme les laboratoires, les chercheurs, et les professionnels de santé impliqués dans l'analyse et la gestion des maladies.

L'utilisation de ces données présente des avantages pour la sécurité publique, mais, dans certains cas, des dérives sont pointées du doigt.

Le programme de santé digitale est mis en œuvre alors que la protection des droits numériques est médiocre, sans compter les menaces croissantes au droit à la vie privée et aux violations des données personnelles, ce qui jette un doute sur l'intégrité du programme.

Les risques liés à l'utilisation des données de santé sont majeurs et particulièrement dangereux pour les patients. Ces principaux risques sont :

- Risques de vol de données de santé : la valeur des données de santé sur le marché noir en fait une cible attrayante pour les cybercriminels. Le vol de ces informations peut conduire à l'usurpation d'identité, à des fraudes médicales, voire à des extorsions. Concernant la sécurité, les tentatives de vol de données de santé sont de plus en plus répandues. En France en 2020, c'est en moyenne un établissement de santé par semaine qui est la cible de tentatives de vol. À l'international, c'est par exemple le cas de l'établissement de santé SingHealth à Singapour qui s'est fait dérober les informations détaillées de 1,5 million de patients, incluant le premier ministre. Ces nombreuses attaques s'expliquent notamment par le fait que la donnée de santé est particulièrement lucrative : un dossier médical peut se revendre entre 50 et 100 dollars sur le dark web, soit en moyenne trois fois plus cher que des données classiques[63].

- Ransomwares et extorsions : les attaques par ransomwares ciblant les systèmes de santé peuvent paralyser les opérations médicales en cryptant les données, exigeant des rançons pour leur libération. Ces attaques compromettent la confidentialité des données et peuvent entraver l'accès aux soins de santé.

- Manipulation de données[64] : la manipulation malveillante des données de santé peut avoir des conséquences graves, notamment en modifiant les dossiers médicaux pour induire en erreur les diagnostics ou les traitements.

[63] Les risques à héberger et exploiter des données de santé (padok.fr).
[64] Walter Hanhart, le dossier Medical informatisé, page 9 : dossier_medical.pdf

- Menaces internes : les cyberattaques ne sont pas uniquement externes ; les menaces internes, qu'elles soient intentionnelles ou résultant d'une négligence, sont également préoccupantes. Ces menaces internes peuvent être la divulgation des données.

Ces risques potentiels pourraient être aggravés lorsque les données sont stockées dans des bases de données centralisées[65] et lorsque les politiques de sécurité de l'information sont inadéquates. C'est notamment le cas lorsque les bases de données sont interconnectées avec d'autres agences gouvernementales et reliées pour fournir des services pratiques. Ou bien lorsque les données de santé sont hébergées à l'étranger.

Ces risques s'ajoutent lorsque les données de santé sont collectées par les tiers intéressées (GAFAM, assureurs)[66]. En effets les « tiers intéressés » - gafam (Google, amazon, facebook, apple et microsoft)., assureurs et autres entreprises innovantes collectent des données de santé et investissent de plus en plus le secteur de la santé. Leurs initiatives sont multiples dans ce domaine. Ils développent parfois une activité en coopération avec des professionnels de santé. Souvenons-nous du partenariat entre le National health system britannique et Alphabet dont l'objet était le traitement des données de 1,6 millions de patients par Deepmind dans le but de mieux détecter les lésions rénales. D'autrefois, leurs initiatives sont autonomes. Alphabet développe ainsi une pluralité de projets : traitement de données de santé, allongement de la vie, prévention et traitement des cancers (Calico), cartographie de la santé humaine (Baseline), développements de dispositifs médicaux connectés ou de robots chirurgicaux (Verily). Facebook, Apple ou des assureurs s'orientent quant à eux vers le suivi de l'activité physique au moyen d'objets connectés. Amazon cherche, de son côté, à développer une assurance santé mais s'intéresse aussi à la détection des cancers[67]. la collecte des données « *de santé* » par les « *tiers intéressés* » serait « d*angereuse* » spécialement en contemplation du « *Big data*»[68]. A. Mendoza-Caminade, « *Big data et données de santé. Cette expression désigne « non seulement l'expansion du volume des données mais aussi celle de la capacité à les utiliser* »[69]. La technique du *Big data* dépendrait d'au moins cinq facteurs : le volume des données traitées, leur variété, la vélocité et la capacité des applications à les traiter notamment en temps réel, leur véracité et enfin la valeur qui peut

[65] Walter Hanhart, le dossier Medical informatisé, page 9 : dossier_medical.pdf
[66] Thibault Douville, Les dangers de la collecte des données de santé par les tiers intéressés (gafam, assureurs…) Dans Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM) 2018/3 (N° 20), pages 12 à 16.
[67] Pour une cartographie, à jour en février 2018, des projets développés par les géants d'internet : https://www.usine-digitale.fr/article/google-amazon-facebook-apple-quels-sont-leurs-projets-dans-la-sante.N646518.
[68] A. Mendoza-Caminade, « Big data et données de santé : quelles régulations juridiques ? », RLDI, n° 127, juin 2016, p. 39 et s., spéc. p. 41 ; C. Castets-Renard, « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », RLDI, n° 111, janvier 2015, p. 38.
[69] Conseil d'État, Le numérique et les droits fondamentaux, Étude annuelle 2014, La documentation française, 2014, p. 48

en être tirée[70]. Son utilisation peut poursuivre une finalité collective, notamment statistique[71], ou individuelle, en permettant le profilage et la fourniture de services personnalisés. Le big data de données de santé par les « tiers intéressés » peut présenter des avantages. En ce sens, bien des arguments pourraient être avancés parmi lesquels la capacité dans laquelle ces acteurs seraient de développer des solutions innovantes et personnalisées au service de la santé humaine, qu'il s'agisse de prévenir les maladies, de les détecter et de les soigner, ou de favoriser le bien-être des personnes. À l'inverse, la puissance économique de ces acteurs, le risque de privatisation de la santé. La remise en cause des politiques publiques ou les risques importants d'atteinte à la vie privée des individus font naître des inquiétudes. Pensons à Grindr, ce site de rencontre qui a collecté et partagé le statut sérologique de ses membres et a rendu ces données publiques[72]. En plus Les « tiers intéressés » échappent aux dispositions sur la sécurité et ne sont soumis qu'aux exigences sécuritaires résultant sur la protection des données à caractère personnel.

V. Recommandations

Pour mieux assurer la sécurité juridique, il est nécessaire d'apporter quelques recommandations afin de mieux garantir la protection des données de santé des citoyens sénégalais.

A. Cadre Normatif

En matière de traitement des données de santé, la loi exige un certain nombre de respect liés au droit de la personne dont les données sont traitées. Les droits reconnus par les différentes législations aux personnes dont ces données à caractère personnel font l'objet d'un traitement constituent le fondement même de la protection desdites données de santé. Ce fondement doit être renforcé lorsqu'on se trouve en face des données de santé. Ces dernières, du fait de leur sensibilité, doivent être particulièrement encadrées par la loi. En plus, le secteur de la santé est, aujourd'hui fortement marqué par l'introduction des technologies. En effet, la logique de la protection des données personnelles doit être revue pour que ces technologies ne soient pas un fléau à cette protection. Il faut préciser que la protection des données personnelles n'est pas seulement une affaire nationale. Elle préoccupe aussi d'autres normes extranationales qui luttent pour une meilleure protection desdites données.

[70] Conseil d'État, ouvr. préc., p. 48

[71] V. sur le lien entre le big data et l'intelligence artificielle en santé : L. Maisnier-Boché, « *Intelligence artificielle et santé* », JDSAM n°17, 2017 p. 25.

[72] hibault Douville, Les dangers de la collecte des données de santé par les tiers intéressés (gafam, assureurs…) Dans Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM) 2018/3 (N° 20), pages 12

Pour ce faire, il est impératif que le cadre législatif actuel, pour le Sénégal et pour l'Afrique, se modernise afin de répondre au mieux au besoin d'encadrement qu'imposent ces traitements de données à caractère personnel issus de ces innovations nouvelles. Or, force est de constater que cette loi qui n'a pas été retouchée par le législateur depuis 2008 méritait d'être modifiée au gré des avancées technologiques. De la même manière, la règlementation supranationale, à savoir l'acte additionnel de la CEDEAO et la convention de Malabo, auraient besoin d'être actualisées.

Aujourd'hui, en tenant compte des avancées technologiques, la rédaction des textes de lois dans nos pays requiert de l'anticipation mais aussi de l'innovation. Cette nécessité de réforme peut être motivée par la coopération et partenariat au niveau africain dont la Commission de protection des Données Personnelles (CDP) préside le Groupe de travail mis en place dans le cadre de l'Alliance Smart Africa. Ce Groupe de travail a pour mission de proposer un cadre harmonisé pour la protection des données et le respect de la vie privée sur la base de la Convention de l'Union Africaine sur la Cybersécurité et la protection des données à caractère personnel (Convention de Malabo), et par l'intégration d'autres cadres internationaux régionaux. C'est pour cette raison que les lois organisant la protection des données personnelles notamment les données sensibles en l'occurrence les données de santé, doivent être réadaptées avec la numérisation des données des patients.

La loi devait, comme ces homologues, en l'occurrence la France, réaménager les formalités anciennes qui prévoyaient de manière générale que les traitements nécessaires à la médecine préventive, des diagnostics médicaux, ou de la gestion des services de santé et mis en œuvre par un membre d'une profession de santé, étaient soumis à une déclaration préalable auprès de la CDP, adopter des formalismes nouveaux, notamment l'obligation de documentation interne à l'organisme responsable du traitement. En outre, en ce qui concerne les traitements susceptibles d'engendrer un risque élevé pour les droits et les libertés fondamentaux, la loi doit exiger une analyse d'impact préalable.

Par ailleurs, la sécurité est un élément clé en matière de protection des données à caractère personnel en plus forte raison lorsqu'on se trouve en face des données sensibles, en l'occurrence des données de santé. Le responsable du traitement a l'obligation de mettre en œuvre des mesures de sécurité afin d'assurer que les données ne sont pas détruites, modifiées ou divulguées indument, que ce soit par accident ou suite à une action malveillante.

En fait, les données de santé présentent des caractéristiques qui justifient des mesures de protection spécifiques, au-delà du cadre général des données personnelles. D'une part, il s'agit de données particulièrement intimes, dont la divulgation peut porter gravement atteinte à la vie privée d'une personne. D'autre part, leurs usages exigent une fiabilité supérieure : s'il est éventuellement admissible

qu'un compte sur un réseau social soit indisponible pendant quelques heures, on ne peut tolérer qu'un dossier médicalisé soit altéré ou inaccessible lors d'une intervention. L'exactitude des données de santé et leur accessibilité sont vitales en cas d'urgence. C'est pourquoi les normes nationales et supranationales en matière de protection des données personnelles doivent instituer des obligations particulières pour l'hébergement de données de santé comme celle de la France.

En effet, l'informatisation des hôpitaux, des cabinets médicaux et paramédicaux, des pharmacies et des laboratoires, devient une réalité dans nos sociétés actuelles. Tant que les données restaient stockées localement, sans connexion à internet, le risque de fuite de données, qu'elle soit accidentelle ou intentionnelle, était faible.

Mais avec le recours croissant aux échanges en ligne entre acteurs de la santé, a la télémédecine et au stockage dans le « *cloud* », les données de santé sont appelées à circuler mondialement et à être hébergées chez de nombreux prestataires. Les risques sont multipliés dans les mêmes proportions. Ces risques sont liés aux fuites de données. Ces dernières peuvent se retrouver en ligne suite à une négligence ou à un accident. Cette fuite de données ne résulte pas d'une malveillance, mais d'une insuffisance de mise en œuvre des règles de sécurité. Des dossiers peuvent ainsi se retrouver référencés par un moteur de recherche comme Google et consultables par tout un chacun.

En tenant compte de cette situation, le législateur doit prendre avec beaucoup de responsabilité la question de l'hébergement des données de santé. Relevant du domaine des données personnelles classées sensibles, leur hébergement doit être pris de manière scrupuleuse afin de répondre à toutes les exigences relatives à la sécurité desdites données.

Ceci doit donner l'idée au législateur de veiller à la procédure d'hébergement afin de garantir la sécurité, la confidentialité, la pérennité et l'accessibilité des données des patients. A ce niveau, la loi doit imposer des obligations aux sociétés et aux organismes qui hébergent des données de santé pour le compte de tiers, qu'il s'agisse des établissements de santé, des professionnels de santé ou des patients. Ainsi, la loi doit instituer la mesure de certification. Dans ce cas les hébergeurs doivent être titulaires d'un certificat de conformité délivré par la commission de la protection des données personnelles(CDP) ou bien par une autre autorité en charge de la question. Ou bien la prestation d'hébergement doit faire l'objet d'un contrat entre le patient et l'hébergeur ou entre le professionnel de santé et l'hébergeur, le consentement du patient étant préalablement recueilli. Afin de permettre à son cocontractant d'exprimer les risques liés à la dématérialisation.

Et en outre, le législateur doit règlementer l'échange et le partage de données de santé entre : l'échange et le partage de données relatives à la santé entre professionnels de santé doivent être limités aux informations strictement nécessaires à la coordination ou a continuité des soins, à la prévention ou au suivi médico-social et social de la personne. Chaque professionnel de santé ne peut, dans ce cas, transmettre ou recevoir que les données qui relèvent du périmètre de ses missions, en fonction de ses habilitations.

Dans le cadre de l'échange ou du partage de données relatives à la santé, des mesures physiques, techniques et administratives de sécurité doivent être adoptées, de même que des mesures nécessaires pour garantir la confidentialité, l'intégrité et la disponibilité de ces données. Enfin, l'Etat du Sénégal doit mettre en place des dispositions relatives aux référentiels de sécurité et d'interopérabilité des données de santé et Interdire de procéder à une cession ou à une exploitation commerciale des données de santé.

B. Cadre Institutionnel

Les autorités chargées de la protection des données doivent disposer des pouvoirs et des ressources nécessaires pour faire respecter le principe de la vie privée aux fins de la collecte. Elles devraient donner des orientations aux fournisseurs et aux prestataires de services sur la nécessité de la transparence et de la responsabilité en ce qui concerne le principe de l'objet de la collecte, en tant que fondement de la confiance des consommateurs. Ensuite, les gouvernements doivent veiller à ce que les autorités de la protection des données disposent des ressources nécessaires pour surveiller et faire appliquer le principe de « *l'objectif de collecte* ».

Ensuite, l'efficacité et l'efficience de la gouvernance des données personnelles passe par une stabilité du cadre institutionnel et la suppression de la multiplicité des pôles de décision. Pour une plus grande cohérence, regroupons au sein d'une même autorité des moyens humains et financiers consacrés au numérique et la création d'une autorité de santé numérique. Cette autorité de santé numérique sera chargée des tâches suivantes :

- Superviser les points de contact nationaux pour la santé numérique et coopérer avec d'autres autorités de santé numérique,
- Assurer, à l'échelon national, la mise en œuvre d'échange des dossiers médicaux électroniques, en coopération avec les autorités nationales et les parties prenantes ;

- Contribuer, au développement d'échange des dossiers médicaux électroniques, ainsi qu'à l'élaboration de spécifications communes traitant des questions d'interopérabilité, de sécurité, de sûreté ou de droits fondamentaux,
- Renforcer les capacités nationales de mise en œuvre de l'interopérabilité et de la sécurité de l'utilisation primaire des données de santé électroniques et participer aux échanges d'informations
- Offrir des services de télémédecine dans le respect de la législation nationale et veiller à ce que ces services soient faciles à utiliser et accessibles à différents groupes de personnes physiques et de professionnels de la santé.

Par ailleurs, le législateur doit imposer dans chaque hôpital une personne chargée de vérifier toutes les questions relatives à la protection des données personnelles de santé. Celui-ci aura comme mission de vérifier la conformité de tout traitement fait sur les données de santé et de gérer aussi les habilitations d'accès aux données des patients. Cette personne, appelée le délégué à la protection des données personnelles, doit informer et conseiller le responsable du traitement ou le sous-traitant ainsi que le personnel des obligations qui leur incombent en vertu de la loi de 2008 sur la protection des données à caractère personnel au Sénégal et de l'ensemble des instruments juridiques en la matière dont leur application s'observe au Sénégal. Ce délégué a aussi pour mission de dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données. Toujours, dans l'exécution de sa mission, le délégué à la protection doit coopérer avec l'autorité de contrôle.

Conclusion

Au terme de cette étude, on doit constater que malgré toutes les réponses juridiques déjà données aux questions posées par l'introduction des nouvelles technologies de l'information et de la communication dans le domaine de la santé, le droit positif est encore loin de résoudre tous les problèmes liés à la protection de la vie privée. Alors, faut-il, pour autant balayer du revers de la main tout le droit existant pour en créer un autre spécifique à cette nouvelle réalité ? Sur la question, les professeurs GAUTRAIS et TRUDEL ne sont pas aussi radicaux. Ils semblent militer en faveur d'une adaptation plutôt qu'un rejet catégorique du droit existant. Selon eux, « face aux bouleversements technologiques que beaucoup considèrent comme, à juste titre, « *révolutionnaires* », il n'est d'autre choix que de changer le droit aussi. Suivant des degrés différents, plusieurs considèrent donc que ce domaine en émergence, à l'instar du droit plus englobant qu'est le droit du cyberespace, est différent du droit traditionnel. Le droit de la vie privée devrait par conséquent être au pire remanié, au mieux rebalancé, certains principes

étant désuets et d'autres sous-évalués ». Nous partageons leur position et considérons que le plus judicieux serait « de concilier situations « nouvelles » et « vieux » droit ». C'est aussi la politique adoptée par le gouvernement sénégalais dans l'encadrement juridique de la gestion électronique des données de santé.

La gestion électronique des données de santé s'inscrit non seulement dans le champ du traitement automatisé des données sensibles, notamment les données de santé. Son encadrement juridique est donc assuré par le droit commun au traitement de toutes les données personnelles tout comme par les règles spécifiques au traitement des données santé.

L'étude a révélé que la protection des données de santé est un droit pour tout citoyen et une responsabilité de l'Etat. Il est donc nécessaire de renforcer le cadre légal et réglementaire de la gestion des données de santé en mettant l'accent sur la coopération interétatique.

La coopération internationale est une nécessité absolue car, en matière de cybercriminalité, on ne peut pas faire cavalier seul. Quand les attaques viennent d'intrus étrangers, une approche multilatérale est indispensable à l'efficacité de la cyber-répression et de la cyberdéfense.

La protection absolue des données de santé est possible. Elle passe par la prise de conscience par les pouvoirs publics de l'enjeu national de la souveraineté numérique et, par conséquent, de l'établissement d'une politique industrielle des réseaux informatiques et de l'Internet.

Il est temps de reconquérir notre souveraineté sur les réseaux, d'y retrouver la maîtrise de nos données. Telle est la souveraineté numérique. L'accomplissement de cet objectif ne dépend pas seulement de notre souveraineté sur internet, mais de notre souveraineté globale.

Liste des références

- **Ouvrages**

DRAME (P.F) et SARR (R), *L'impact du règlement sur la protection des données (RGPD) en Afrique*, Harmattan, 2021, 251 p.

KAMTO (M), *Droit international de la gouvernance*, Editions A. PEDONE, 2013, 338 p.

LO (M), *La protection des données à caractère personnel en Afrique, Réglementation et régulation*, Baol Editions, 2017, 267 p.

DANIEL (P), *Le droit des technologies de l'information au Québec*., LexisNexis Canada, 29 février 2008, 236 p.

THIONGANE (O), *Les promesse du numérique,* Editions Sédar, 134 p.

TOURE (P.A.), *Le traitement de la cybercriminalité devant le juge : L'exemple du Sénégal*, Harmattan 2014, 616 p.

- **Articles**

Castets-Renard (C), « *Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data »*, RLDI, n° 111, janvier 2015, p. 38.

Douville (T), « *Les dangers de la collecte des données de santé par les tiers intéressés (gafam, assureurs…)* » Dans Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM) 2018/3 (N° 20), pages 12 à 16.

MICHEL(L). Secret médical et dossier informatisé. Louvin médical n° 120. Belgique 2001. p. S131

Mendoza-Caminade (A), *« Big data et données de santé : quelles régulations juridiques* ? », RLDI, n° 127, juin 2016, p. 39 et s., spéc. p. 41 ;

Maisnier-Boché (L), *« Intelligence artificielle et santé* », JDSAM n°17, 2017 p. 25.
Walter (H), « *le dossier Médical informatisé* », page 9 : dossier_medical.pdf

SAKHO (A), « article publié Sud Quotidien » : « « Le numérique n'est pas un secteur d'activité, mais une forme d'expression de l'économie », le 7 juin 2017, disponible sur le : https://www.osiris.sn/Abdoulaye-SakhoProfesseur-agrege.html.

- **Les textes**

Convention n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel signée à Malabo en Guinée équatoriale le 27 juin 2014.

Acte additionnel 1/01/ 10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO.

Loi n° 2008-12 du 25 janvier 2008, sur la protection les données à caractère personnel (JORS, n°6406, du 3 mai 2008, p.434).

Loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal (JORS n°6975).

Loi n° 2008-41 du 20 aout 2008 sur la Cryptologie ainsi que par Ie décret d'application n" 2010-1209 du 13 septembre 2010 modifié et complété par Ie décret n" 2012-1508 du 31 décembre 2012.

Décret n° 2008-721 du 30 juin 2008, portant application de la loi 2008-12 du 25 janvier 2008 sur la protection les données à caractère personnel (JORS, n° 6443 du 20 décembre 2008).

- **Web**

France ASSOS Santé, Secret médical : respect, partage, dérogation et violation : Le Secret médical - Définition (partagé...), Violation, Dérogation (france-assos-sante.org).
Sénégal-Accès à l'information: les limites bien fixées en milieu médical : Sénégal-Accès à l'information: les limites bien fixées en milieu médical - Une information fiable et indépendante sur... (ouestaf.com).
Secret médical : de quoi s'agit-il ? | Service-Public.fr
Secret médical : « Un médecin ne doit pas divulguer la maladie de son patient » : Secret médical : « Un médecin ne doit pas divulguer la maladie de son patient » (MackySall) (senego.com)