



DONNÉES DE SANTÉ : **PASSER LE CAP CITOYEN !**

**AU SERVICE D'UNE MEILLEURE GOUVERNANCE
ET PLUS GRANDE EFFICIENCE DU SYSTÈME DE SANTÉ**

JUIN 2021
POLITIQUES, INSTITUTIONS ET DÉMOCRATIE



TABLE DES MATIÈRES

INTRODUCTION _____ 4

PARTIE 1 - LES DONNÉES NUMÉRIQUES : UNE NOUVELLE DONNE POUR LA GOUVERNANCE DU SYSTÈME DE SANTÉ ? _____ 14

De l'hétérogénéité des données dans la chaîne
de valeur de la santé... _____ 18

...À une gouvernance peu lisible de ces données _____ 35

Des données dont la sensibilité accentue la complexité _____ 44

PARTIE 2 - POUR UNE CULTURE DES DONNÉES DE SANTÉ PARTAGÉE _____ 60

Acculturer les acteurs du secteur de la santé
aux données numériques _____ 61

Sensibiliser le secteur numérique aux enjeux propres
aux données de santé _____ 74

PARTIE 3 - REDÉFINIR LA GOUVERNANCE DES DONNÉES POUR UN SYSTÈME DE SANTÉ PLUS EFFICIENT ET PLUS DÉMOCRATIQUE _____ 76

Clarifier le pilotage de la politique publique
des données de santé _____ 77

Des arbitrages techniques et juridiques indispensables _____ 83

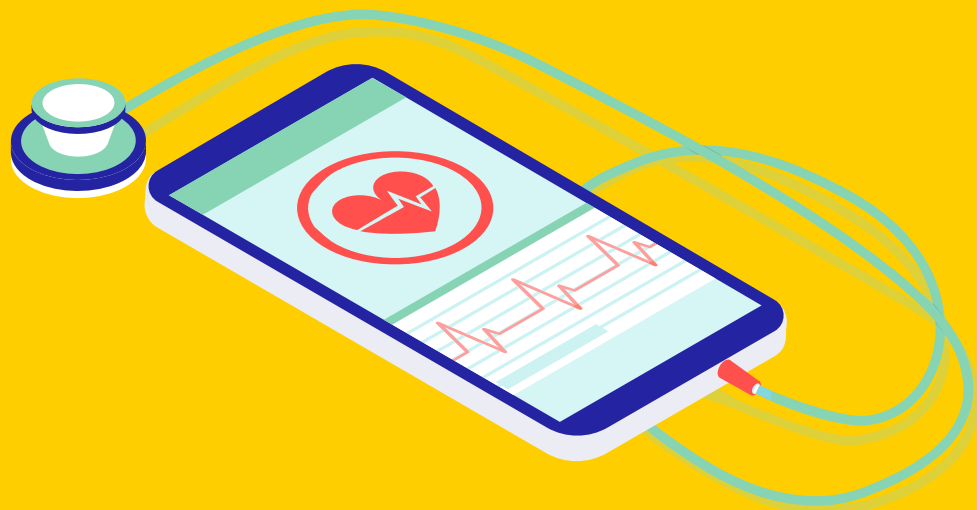
Mettre le citoyen au cœur de la gouvernance
des données de santé _____ 95

CONCLUSION _____ 101

LES PRÉCONISATIONS DE RENAISSANCE NUMÉRIQUE _____ 104

GLOSSAIRE _____ 106

INTRODUCTION



UN CONSENSUS PARTAGÉ SUR L'UTILITÉ DES DONNÉES NUMÉRIQUES POUR LE SYSTÈME DE SANTÉ

S'il est une chose que la pandémie de Covid-19, qui touche le monde depuis plus d'un an, aura su démontrer, c'est l'utilité de disposer de données fiables et à jour pour gérer un système de santé en cas de crise. Sans les remontées quotidiennes de données en provenance des hôpitaux, des établissements d'hébergement pour personnes âgées dépendantes (EHPAD), des laboratoires de biologie et autres établissements de santé, le développement d'indicateurs permettant de guider les prises de décision publiques (confinement, déconfinement, couvre-feu, etc.), à l'instar du taux d'incidence¹, du taux de reproduction² ou du niveau de tension hospitalière³, n'aurait pas été possible. Dans le domaine de la santé comme dans de nombreux autres domaines, les données constituent un réel outil de pilotage et de gestion. Elles sont également une composante importante de la transparence des décisions prises par les pouvoirs publics et du contrôle de l'efficacité de ces dernières. La plateforme dashboard.covid19.data.gouv.fr permet, par exemple, à tout un chacun de consulter l'évolution de la situation épidémique (nombre de nouveaux patients hospitalisés, de personnes admises en réanimation, de doses de vaccin injectées, etc.) et de visualiser l'ensemble des données disponibles sous forme de cartes. L'utilité du partage et de l'exploitation des données dans le champ de la santé va, toutefois, bien au-delà de la gestion de crise, et si les impératifs liés à la lutte contre l'épidémie de Covid-19 sont venus renforcer l'intérêt pour les données de santé, le lien entre les données et la santé précède très largement la transformation numérique du secteur. À condition qu'elles soient utilisées avec toutes les garanties que leur sensibilité exige, ces données peuvent être mobilisées afin d'améliorer et fluidifier les parcours de soins, développer la télémédecine, faire progresser la recherche scientifique, notamment épidémiologique, piloter le système de santé, ou même développer la médecine préventive⁴ qui, malgré les priorités qui lui sont accordées, fait aujourd'hui défaut.

¹ Nombre de cas par semaine pour 100 000 habitants.

² Nombre de personnes contaminées par un malade.

³ Nombre de lits de réanimation occupés par les patients Covid19 par rapport au nombre de lits fin 2018.

⁴ Ces finalités sont celles qui ont été le plus souvent citées par les acteurs interrogés dans le cadre de ce rapport.

C'est dans cette optique que s'inscrit la stratégie nationale « Ma Santé 2022 », et plus particulièrement son volet « Accélérer le virage numérique », qui a vu le jour en mai 2019 sous la forme d'une feuille de route. Portée par le ministère des Solidarités et de la Santé, cette dernière s'articule autour de cinq objectifs : renforcer la gouvernance du numérique en santé, intensifier la sécurité et l'interopérabilité des systèmes d'information en santé, accélérer le déploiement des services numériques socles, déployer au niveau national des plateformes numériques de santé, et enfin soutenir l'innovation et favoriser l'engagement des acteurs⁵. Cinq objectifs au cœur desquels se trouvent les données de santé.

Certains de ces enjeux se sont retrouvés dans le Ségur de la santé, la consultation des acteurs du système de soins français qui s'est tenue entre le 25 mai et le 10 juillet 2020. Ces négociations sont nées notamment des tensions durables au sein du système de santé, et en particulier la situation difficile dans laquelle se trouvent les hôpitaux, révélées avec une plus vive acuité par l'épidémie de Covid-19. Manque de lits et de personnels, financements inadaptés, décisions descendantes et éloignées de la réalité du terrain, cloisonnement entre médecine de ville et hôpital, entre les domaines sanitaire et médico-social, complexité du cadre normatif, manque de pertinence de certains soins⁶, sont autant de points d'alerte qui ont été relevés par les acteurs du système de santé à l'occasion de ce Ségur⁷. S'ils visent à répondre à ces problématiques urgentes, en particulier en revalorisant les métiers des établissements de santé et des EHPAD, les accords issus du Ségur de la santé ont également vocation à « *accélérer dans tous les domaines de la transformation de notre système de santé.* »⁸ Ainsi, le plan France Relance annoncé par le Premier ministre Jean Castex le 15 juillet 2020 et à travers lequel les conclusions du Ségur de la santé se matérialisent, prévoit d'allouer 6 milliards d'euros au secteur de la santé, dont 2,1 milliards sur cinq ans dédiés à « *la transformation, la rénovation, l'équipement et le rattrapage numériques des établissements médico-sociaux* », et 1,4 milliard sur trois ans en vue de « *[rattraper le] retard dans l'interopérabilité*

et la modernisation des outils numériques en santé »^{9,10}. En outre, 136 millions d'euros seront spécialement dédiés aux enjeux de cybersécurité, dont une partie ciblée spécifiquement vers les établissements de santé.

Au niveau européen, cette ambition de transformer, par le numérique et par les données, le système de santé, s'incarne notamment au travers de la stratégie pour les données présentée par la Commission européenne le 19 février 2020, qui prône la mise en place d'un espace commun européen des données de santé¹¹.

Le constat selon lequel il convient de mettre le potentiel des données au service du système de santé et des citoyens est ainsi largement partagé au sein de l'Union européenne, comme en attestent également les différentes initiatives en cours et les investissements massifs consentis en ce sens (renforcés par la crise sanitaire). Mais bien que ces données existent en abondance, et malgré les grands chantiers enclenchés, les acteurs de la chaîne de santé ne sont pas parvenus à s'en saisir pleinement pour améliorer le système et le rendre plus efficient et plus démocratique.

DES ACTIFS HAUTEMENT SENSIBLES, DONT L'EXPLOITATION SOULÈVE DE NOMBREUSES QUESTIONS

Si le partage et l'exploitation des données dans le champ de la santé portent de nombreuses promesses, il ne faut pas négliger leur caractère hautement sensible. Depuis 2018, le RGPD définit les données de santé comme des « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé,*

5 Ministère des Solidarités et de la Santé, Dossier d'information « Accélérer le virage numérique », Feuille de route stratégique du numérique en santé, mai 2019 : https://esante.gouv.fr/sites/default/files/media_entity/documents/Dossier_virage_numerique_masante2022.pdf

6 Est particulièrement remise en cause la tarification à l'acte, qui mène à une multiplication des actes médicaux inadéquats ou inutiles. Afin de renforcer la pertinence des soins, Olivier Véran propose d'étendre la rémunération sur objectifs de santé publique à d'autres spécialités que la médecine généraliste.

7 Discours d'Olivier Véran, Conclusions du ségur de la santé, 21 juillet 2020 : https://solidarites-sante.gouv.fr/IMG/pdf/200721_-_discours_d_olivier_veran_-_conclusions_du_segur_de_la_sante.pdf

8 Ibid.

9 Ministère de l'Économie, des Finances, et de la Relance, Plan massif d'investissement en santé : https://www.economie.gouv.fr/files/files/directions_services/plan-de-relance/plan-massif-investissement-sante.pdf

10 Sur ces 1,4 milliard, 800 millions seront consacrés à l'intégration des prérequis techniques pour la modernisation, l'interopérabilité, la réversibilité et la sécurité des systèmes d'information (SI) de santé, 200 millions au renforcement des équipes numériques et aux prestations d'accompagnement au sein des opérateurs concernés (notamment l'Agence du numérique en santé et l'Assurance Maladie), et 400 millions au soutien à la circulation des données de santé.

11 Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité Économique et Social européen et au Comité des Régions, « Une stratégie européenne pour les données », COM(2020) 66 final, 19 février 2020, pp. 35-36 : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>

qui révèlent des informations sur l'état de santé de cette personne »¹². Cette définition rejoint l'acception large de l'Organisation mondiale de la santé (OMS), qui définit la santé comme « *un état de complet bien-être physique, mental et social* ». Ce rapport aborde la santé dans cette même acception et non comme l'absence ou la présence d'une pathologie. Dans cette optique, le terme de « citoyen » est préféré à celui de « patient » ou « d'utilisateur ». Le champ des données de santé est ainsi très vaste. Au-delà des données dites « médicales », recueillies dans le cadre du parcours de soins par les professionnels de santé, cette notion englobe, par exemple, les données issues d'objets connectés (montres, bracelets, balances, etc.) qui, en fonction de leurs usages, peuvent être considérées comme des données de santé. Ces données révèlent des informations relatives à l'état de santé. En cela, elles touchent à ce qu'il y a de plus intime chez les individus, et revêtent une sensibilité particulière.

Du fait de cette sensibilité, le partage et l'exploitation des données de santé soulèvent des questions éthiques importantes. Est-il acceptable, par exemple, de vendre ces données et, le cas échéant, à quelles conditions ? L'exploitation de ces données, qui entraîne le développement de nouveaux outils dits du « numérique en santé », ne risque-t-elle pas, à l'heure où une personne sur six n'utilise pas Internet en France¹³, de renforcer les inégalités d'accès aux soins ?... Si nous entendons passer un cap dans l'exploitation des données dans le domaine de la santé, que ce soit dans le cadre du parcours de soins ou à des fins de recherche scientifique, ces questions méritent une attention collective, et l'ensemble des acteurs de la chaîne de santé doivent être impliqués dans ce débat.

DE LA NÉCESSITÉ DE QUESTIONNER LA GOUVERNANCE ET LES CONDITIONS DE PARTAGE DES DONNÉES DE SANTÉ

Ces enjeux sont au cœur des travaux de Renaissance Numérique, qui s'est historiquement investi dans les sujets liés à la transformation numérique du

système de santé, cette dernière revêtant une dimension particulièrement citoyenne. Ainsi, dès 2014, le think tank publiait un livre blanc¹⁴ sur la transformation numérique du secteur, et formulait seize propositions pour assurer la transition d'un système de santé curatif vers un modèle préventif. Plus de six ans plus tard, force est de constater que cette transition n'a pas eu lieu. À l'approche des élections présidentielles de 2017, Renaissance Numérique s'est à nouveau saisi du sujet, à travers un rapport consacré à la e-santé, détaillant des propositions pour développer une ambition politique en la matière¹⁵. Cette nouvelle publication avait vocation à nourrir les réflexions sur ce qui deviendrait ensuite le volet numérique de la stratégie nationale « Ma Santé 2022 ».

Dans le prolongement de ces travaux, Renaissance Numérique a lancé en février 2020 un groupe de travail dédié à la gouvernance et aux conditions de partage des données de santé. Du fait de leur nature hautement sensible et de leurs caractéristiques inhérentes – elles sont extrêmement hétérogènes, souvent peu interopérables, et parfois porteuses d'une très grande valeur –, les données de santé constituent des actifs difficiles à gouverner. Une difficulté renforcée par la diversité de plus en plus grande des acteurs impliqués dans leur production, leur collecte, leur partage et leur réutilisation. Le terme de « gouvernance » pouvant être l'objet d'interprétations diverses, il est important de noter qu'il est entendu ici comme ce qui « *détermine qui prend les décisions, comment elles sont prises et comment les décideurs sont tenus responsables en ce qui a trait à la collecte, l'utilisation, le partage ou le contrôle des données* »¹⁶ de santé. Derrière le sujet de leur gouvernance, aller vers une plus grande exploitation des données de santé soulève également de nombreuses questions techniques (interopérabilité, cybersécurité) et juridiques (protection de la vie privée et des données personnelles), liées aux conditions de leur partage.

Durant plus d'un an, un groupe de travail a ainsi réuni une douzaine d'adhérents du think tank – chercheurs, professionnels de santé, juristes,

12 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après Règlement général sur la protection des données ou « RGPD »), Article 4(15).

13 Insee, « Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base », Insee Première No 1780, 30 octobre 2019 : <https://www.insee.fr/fr/statistiques/4241397>

14 Renaissance Numérique (2014), *D'un système de santé curatif à un modèle préventif grâce aux outils numériques*, 119 pp. : <https://www.renaissancenumerique.org/publications/d-un-sys-teme-de-sante-curatif-a-un-modele-preventif-grace-aux-outils-numeriques>

15 Renaissance Numérique (2017), *17 Experts / 36 propositions pour une ambition politique en matière de e-santé*, 44 pp. : https://www.renaissancenumerique.org/system/attach_files/files/000/000/104/original/E-Sante-Renaissance_Nume%CC%81rique.pdf?1493195779

16 Coutts, S., Gagnon-Turcotte, S., Sculthorp, M. (2021), « Les partenariats de données numériques », p. 33 : https://downloads.ctfassets.net/e4wa7sgik5wa/6mV2HLHbhKbU2sgtXSTMQX/e769babb86049cd1c5f73e8ba6aebcla/Digital_Data_Partnerships_Report-FR.pdf

industriels de la santé et du numérique –, qui ont mis leurs expertises en commun afin d'aboutir à des recommandations concrètes sur ces questions. Outre cette démarche interne, le think tank a également interrogé des acteurs susceptibles d'apporter un retour d'expérience sur le sujet, à travers la réalisation d'une série d'auditions représentative de la diversité de la chaîne de valeur des données de santé, y compris au niveau européen. Près de quarante acteurs clés, représentant à la fois le secteur public, privé et la société civile, ont ainsi contribué aux réflexions présentées ici¹⁷. Cette démarche multidisciplinaire permet aujourd'hui à Renaissance Numérique de présenter des pistes d'actions adressées à l'ensemble des acteurs du système, afin de faire des données un pilier de la transformation du système de santé. Si elles ont permis de nourrir leurs réflexions, ces auditions ont également conforté les membres du groupe de travail dans l'idée que cet exercice était nécessaire, afin de favoriser la diffusion d'une culture des données dans le domaine de la santé. Certains acteurs ont, en effet, encore des difficultés à appréhender le sujet des données de santé et à s'en saisir. Les questions liées à leurs conditions de partage et à leur gouvernance soulèvent pourtant des interrogations qui exigent une attention de leur part.

UN NOUVEL ÉLAN POUR LA DÉMOCRATIE SANITAIRE ?

La réflexion présentée ici interroge le cadre général de la « démocratie sanitaire » du système de santé français. Sanctuarisée dans le titre III de la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé¹⁸, cette notion renvoie au fait d'associer « *l'ensemble des acteurs du système de santé dans l'élaboration et la mise en œuvre de la politique de santé, dans un esprit de dialogue et de concertation* »¹⁹. Cet effort passe notamment par l'organisation de débats publics, ainsi que par la promotion des droits des citoyens en matière de santé. Si les différents acteurs de la chaîne de santé parviennent à s'en saisir, les données de santé pourraient contribuer à donner un nouveau souffle à ce cadre de la démocratie sanitaire qui peine à s'incarner. Comment redéfinir dès lors la démocratie sanitaire à l'ère des don-

nées de santé ? Patients et associations de patients, citoyens, professionnels de santé, administration centrale, Assurance Maladie, agences régionales de santé (ARS), établissement de santé, collectivités, mutuelles, industrie de la santé, acteurs du numérique, start-ups... tous doivent être considérés dans la gouvernance du système, ce qui nécessite une prise en compte de l'évolution des rôles et des responsabilités de chacun tout au long de la chaîne de santé. Les patients deviennent tour à tour utilisateurs, contributeurs, évaluateurs, voire soignants ou experts grâce à des dispositifs médicaux toujours plus connectés. Les professionnels de santé et les acteurs du médico-social voient leur rôle évoluer avec l'appui de nouveaux outils d'aide à la décision clinique, à l'instar de l'imagerie ou de la biologie. De leur côté, les acteurs du numérique investissent de plus en plus le champ de la santé. Dans cet environnement en constante évolution, comment peut-on assurer une gouvernance lisible et efficace des données de santé ? Cette question soulève deux enjeux.

D'une part, il s'agit de mieux appréhender²⁰ ces données. Utilisées correctement, ces données pourraient, par exemple, être mobilisées afin de contrôler l'efficacité des réformes en matière de santé publique²¹, voire même l'efficacité du système de santé lui-même (délais de prise en charge, qualité des soins, etc.). Une telle démarche pourrait permettre non seulement d'intégrer davantage l'ensemble des maillons de la chaîne de santé, jusqu'aux citoyens, dans la gouvernance du système de santé, mais également d'assister les corps intermédiaires du système (par exemple, les associations de patients) dans leurs actions. Faire des données un levier de la gouvernance du système de santé nécessite toutefois que tous les acteurs de la chaîne soient mis en capacité de se saisir des enjeux du « numérique en santé » ; ce qui n'est pour l'heure pas le cas. En outre, les auditions menées dans le cadre de cette étude ont démontré que les « nouveaux entrants » qui investissent le champ de la santé, issus du monde numérique et souvent incarnés par des start-ups, ne sont pas toujours sensibilisés aux problématiques qui sous-tendent ce secteur. S'assurer de l'adéquation de l'innovation à des besoins spécifiques identifiés au sein du système de santé est pourtant primordial.

20 Au sens de les saisir par l'entendement, la pensée.

21 Comme rappelé dans le rapport *Pour une politique publique de la donnée* élaboré par la « mission Bothorel » et rendu public en décembre 2020, « la donnée est un moyen d'évaluer correctement nos politiques publiques. D'une part, faire de la "data", ce n'est jamais que fiabiliser et permettre en temps réel le bon vieux contrôle de gestion ; et c'est aussi se donner enfin les moyens de suivre l'exécution des dépenses publiques. », p. 7 : https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publicque_de_la_donnee_-_23.12.2020_0.pdf

17 Pour la liste des personnes auditionnées, voir la rubrique « Remerciements » du présent rapport.

18 LOI n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. Accessible en ligne : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000227015/>

19 Agence Régionale de Santé, « Qu'est-ce que la démocratie sanitaire ? », 3 octobre 2018 : <https://www.ars.sante.fr/quest-ce-que-la-democratie-sanitaire-10#:~:text=Faire%20vivre%20la%20d%C3%A9mocratie%20sanitaire,individuels%20et%20collectifs%20des%20usagers>

D'autre part, il s'agit de clarifier leur gouvernance. Du fait de la grande hétérogénéité qui caractérise les données de santé et de la multitude d'acteurs impliqués, cette gouvernance est relativement peu lisible. Or, seule une gouvernance claire des données de santé peut favoriser leur bon partage, c'est-à-dire un partage sécurisé et fluide, qui respecte les droits fondamentaux des citoyens et ne soit pas empêché par les logiques de thésaurisation des données par lesquelles pourraient être tentés certains acteurs de la chaîne de santé.

In fine, passer un cap dans l'exploitation des données de santé tout en s'inscrivant dans le principe de la démocratie sanitaire nécessite non seulement des efforts d'acculturation, mais également des arbitrages d'ordre politique, technique et juridique dans le cadre d'une gouvernance clarifiée.

Il convient de noter enfin que si les réflexions du think tank ont été initiées en amont du pic de la crise sanitaire, cette dernière a rebattu les cartes à certains égards. Des changements en marche forcée, comme le recours massif aux téléconsultations et le remboursement intégral de ces dernières jusqu'à la fin de l'état d'urgence sanitaire²², ainsi que l'extension des cahiers des charges en matière de télésurveillance, ou encore la mise en place des plateformes SI-DEP²³ et Contact-COVID²⁴, n'étaient ainsi pas anticipés. La crise a également entraîné l'accélération du déploiement de certains outils liés au numérique en santé, à l'instar de la plateforme nationale des données de santé (*Health Data Hub*), lancée en avance de phase afin de faciliter le traitement de données relatives au virus²⁵. Enfin, le portage politique,

de même que les choix technologiques mis en œuvre pour développer ces outils, notamment le *Health Data Hub* et l'ancienne application de traçage des cas contact StopCovid²⁶, ont fortement polarisé les débats autour des enjeux liés aux données de santé. Autant que possible, ce rapport prend en compte les développements les plus récents à cet égard. Alors qu'elles ont été propulsées sur le devant de la scène tout au long de l'année qui vient de s'écouler, comprendre les nombreux enjeux que les données de santé soulèvent, ainsi que les opportunités que leur exploitation représente pour notre système de santé apparaît plus que jamais comme une nécessité.

22 Assurance maladie, « Covid-19 : tout savoir sur la téléconsultation et les actes à distance », 9 novembre 2020 : <https://www.ameli.fr/paris/assure/actualites/covid-19-tout-savoir-sur-la-teleconsultation-et-les-actes-distance>

23 Pour « Système d'Informations de DEPIstage ». Il s'agit de la plateforme sécurisée où sont systématiquement enregistrés les résultats des laboratoires de tests Covid-19.

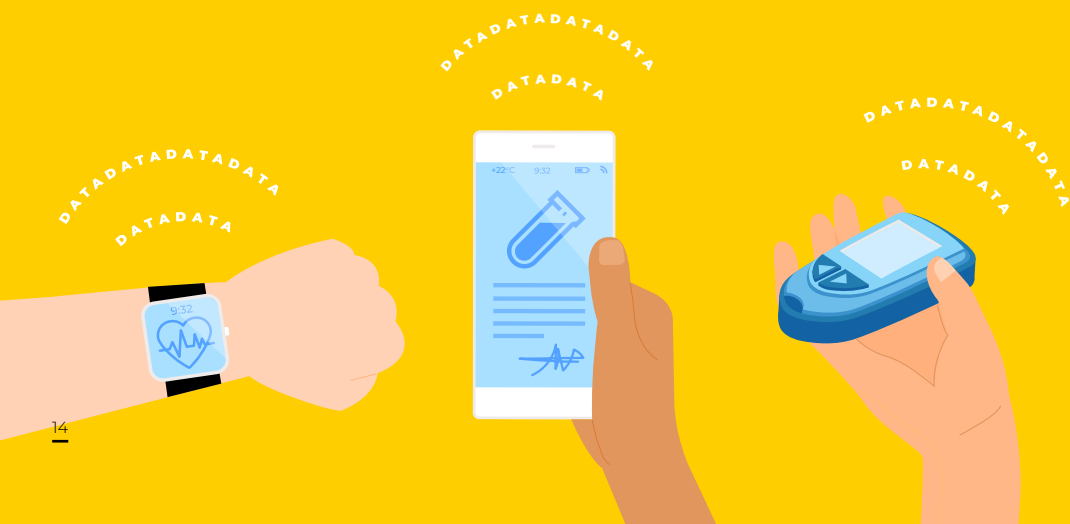
24 Comme indiqué sur le site web du ministère des Solidarités et de la Santé, Contact-COVID est « un outil numérique utilisé par tous les professionnels de santé (médecins, pharmaciens, biologistes des laboratoires de dépistage COVID, et les professionnels habilités par la CNAM, SpF et l'ARS), qui aide à la prise en charge des cas Covid-19. Il permet d'aller au plus vite dans l'identification des personnes-contacts autour d'un cas Covid-19. Il permet de vérifier que chacun a été appelé, informé, testé, et accompagné. »

25 Cette mise en place accélérée a été décrétée par l'arrêté du 21 avril 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de Covid-19 dans le cadre de l'état d'urgence sanitaire : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041812657/>. Elle a notamment permis le raccordement de premières données de santé sur l'épidémie de Covid-19.

26 La première version de l'application, baptisée StopCovid, a évolué au mois d'octobre 2020 vers une nouvelle version enrichie et plus interactive : TousAntiCovid.

PARTIE 1

LES DONNÉES NUMÉRIQUES : UNE NOUVELLE DONNE POUR LA GOUVERNANCE DU SYSTÈME DE SANTÉ ?



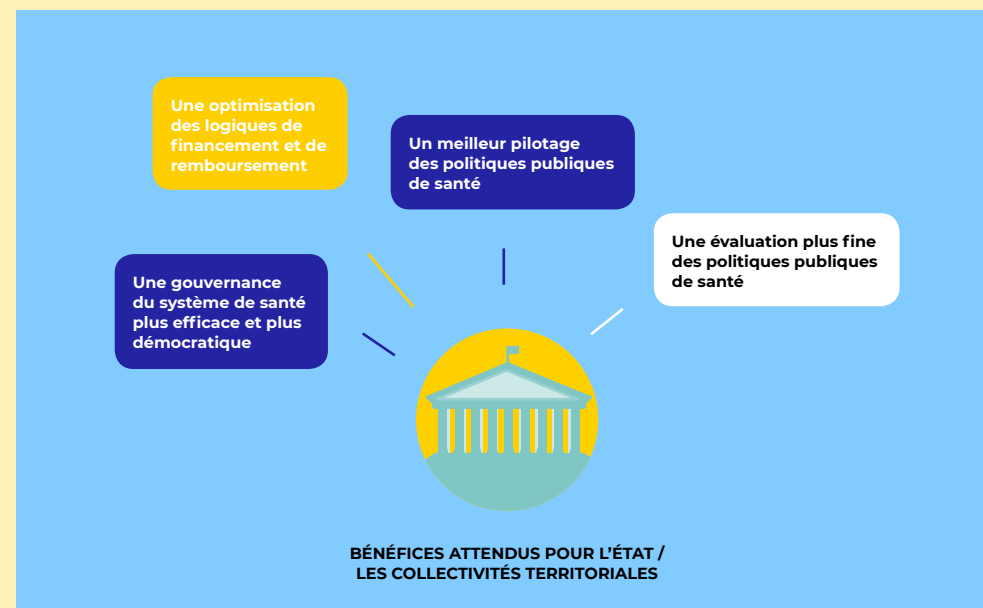
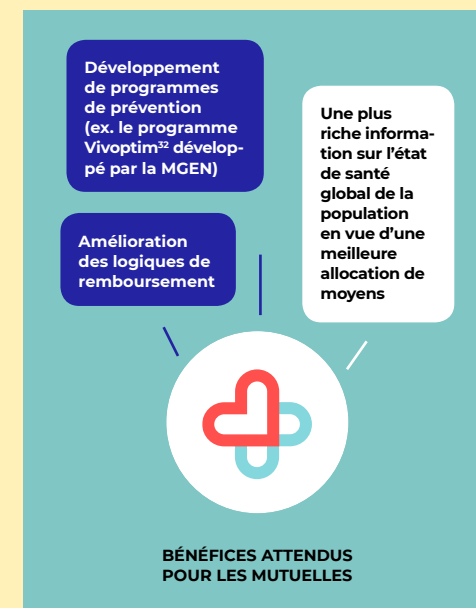
Si le développement accéléré des technologies numériques confère à la notion de donnée dans le domaine de la santé une nouvelle acuité, la santé est historiquement un domaine riche en données. C'est particulièrement le cas en France, où des bases de données nationales contenant des données de millions d'individus ont été mises en place dès les années 1990. Ainsi, le Système national d'information interrégimes de l'Assurance Maladie (SNIIRAM), créé par la loi de financement de la sécurité sociale en 1999, vise quatre grandes finalités : améliorer la qualité des soins, contribuer à une meilleure gestion de l'Assurance Maladie et des politiques de santé, et transmettre aux prestataires de soins les informations pertinentes relatives à leur activité²⁷.

Les bénéfices attendus du partage et de l'exploitation des données de santé sont bien connus et font l'objet d'un relatif consensus, comme l'a démontré la série d'auditions menée dans le cadre de l'élaboration du présent rapport. Il s'agit :

- **d'améliorer les parcours de soins et leur coordination** : fournir le bon soin au bon moment, améliorer la pertinence des soins, fluidifier les parcours de soins ;
- **de faire progresser la recherche scientifique** : améliorer l'efficacité des médicaments et dispositifs médicaux, réduire les effets secondaires indésirables, développer des algorithmes d'aide au diagnostic ou à la décision ;
- **de piloter le système de santé « par les données »** : élaborer et réviser les politiques publiques en se basant sur des données, utiliser les données à des fins d'organisation logistique des établissements de santé et d'évaluation de la qualité et de la pertinence des soins ;
- **de faire progresser la médecine préventive** : au lieu d'une médecine purement curative, évoluer vers une médecine qui aille vers les citoyens de façon proactive (prévention des comportements à risque, encouragement au dépistage de certaines pathologies et aux comportements vertueux, etc.).

²⁷ Code de la sécurité sociale, article L161-28-1.

SCHÉMA 1 - LES BÉNÉFICES ATTENDUS DE L'EXPLOITATION DES DONNÉES NUMÉRIQUES DE SANTÉ



Si l'utilité des données numériques dans le champ de la santé n'est plus à démontrer, accroître leur exploitation dans le cadre des parcours de soins ou à des fins de recherche soulève encore de nombreux enjeux d'ordre économique, politique, juridique et technique. Aborder ces questions nécessite de bien appréhender cet objet complexe que sont les données de santé. Qu'entend-on exactement par « données de santé » ? Par qui sont-elles produites ? Quel cadre juridique encadre leur partage et leur utilisation ?

DE L'HÉTÉROGÉNÉITÉ DES DONNÉES DANS LA CHAÎNE DE VALEUR DE LA SANTÉ...

S'il a fallu attendre 2018 et l'entrée en vigueur du RGPD pour disposer d'une définition légale, applicable en droit français, des données à caractère personnel concernant la santé, cela ne signifie pas pour autant que ces dernières n'existaient pas et ne faisaient pas l'objet de traitements strictement réglementés auparavant.

UNE DÉFINITION JURIDIQUE LARGE DES DONNÉES DE SANTÉ, QUI EN FAIT UN PAYSAGE EXTRÊMEMENT HÉTÉROGÈNE

LES DONNÉES À CARACTÈRE PERSONNEL CONCERNANT LA SANTÉ : UNE DÉFINITION LARGE, CONSACRÉE PAR LE RGPD

Conformément à l'article 4 du RGPD, les « données concernant la santé » sont « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ». Cette définition est très large et ne se limite pas aux seules données médicales telles que définies à l'article L1111-7 du Code de santé publique²⁸.

Elle englobe, comme précisé au considérant 35 du RGPD :

- « *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). »*

Compte tenu de la définition très large du RGPD, la qualification d'une information en « donnée personnelle concernant la santé » au sens du règlement doit faire l'objet d'une analyse au cas par cas. Une donnée peut être une donnée de santé par nature, par croisement ou par destination. Les données de santé dites « par nature » sont les données qui sont intrinsèquement et de manière évidente des données de santé. Par exemple, les résultats d'un examen biologique, les comptes-rendus de consultation ou les traitements suivis par une personne constituent des données de santé « par nature ». Il existe ensuite des données qui, prises indépendamment, ne constituent pas des données de santé, mais qui, lorsqu'elles sont croisées avec d'autres, peuvent donner une indication sur l'état de santé d'une personne. Il s'agit des données de santé « par croisement ». Le poids d'une personne, en soi, ne constitue pas une donnée de santé. S'il est croisé avec la taille de cette personne, en revanche, il est possible de calculer son indice de masse corporelle (IMC), ce qui permet de déduire une information sur son état de santé. Enfin, il existe des données de santé « par destination », qui deviennent des données de santé en raison de leur utilisation à des fins médicales.

Si un individu remplit tous les jours un carnet avec la liste des aliments qu'il consomme, les informations recueillies dans ce carnet ne constituent pas des données de santé. Si, en revanche, cet individu transmet son carnet à un professionnel de santé dans le cadre de son parcours de soins, alors les informations qu'il contient deviennent des données de santé. Les données de santé forment donc une catégorie extrêmement hétérogène de données, dont la nature juridique varie selon qu'elles sont produites dans le cadre du parcours de soins ou en dehors, mais aussi en fonction de l'intention prêtée à la personne qui va traiter ces données.

De cette grande hétérogénéité découle non seulement une certaine difficulté à appréhender les données de santé, à saisir ce qu'elles sont exactement et ce à quoi elles peuvent servir, mais également un degré de complexité important en matière de gouvernance. Du fait de l'acceptation large des données de santé mise en avant dans le RGPD, les acteurs impliqués dans leur production, leur collecte, leur partage et leur utilisation sont extrêmement nombreux : détenteurs, utilisateurs, intermédiaires, autorités et organismes de réglementation, bénéficiaires, etc. Se familiariser avec les données de santé nécessite dès lors de se familiariser avec ces acteurs et avec l'écosystème interconnecté qu'ils constituent.

TABLEAU 1 - TYPOLOGIE GÉNÉRALE DES DONNÉES DE SANTÉ

 Il est important de noter que cette typologie n'est qu'une des typologies possibles des données de santé. Si le choix de catégorisation effectué ici est celui de la source (ou du « producteur ») des données, ces dernières pourraient très bien être catégorisées selon leur finalité, leur statut juridique, leur fonction, leur format ou leur degré d'ouverture (allant des données privées aux données ouvertes en libre accès). Les différentes catégories de données évoquées ci-dessous sont par ailleurs poreuses et

non-exclusives : certaines données peuvent se trouver dans plusieurs catégories du tableau. Selon la Haute Autorité de Santé (HAS), par exemple, les données de vie réelle incluent les données médico-administratives. De la même manière, ces données peuvent constituer des données scientifiques. Enfin, ni les exemples, ni les listes de « producteurs »/« collecteurs » de données évoqués dans le tableau ne se veulent exhaustifs.

Catégorie	Définition	Exemples	Produites / Collectées par...
Données médicales	Les données médicales d'un patient incluent « l'ensemble des informations concernant sa santé détenues, à quelque titre que ce soit, par des professionnels de santé, par des établissements de santé par des centres de santé, par le Service de santé des Armées ou par l'Institution nationale des Invalides, qui sont formalisées ou ont fait l'objet d'échanges écrits entre professionnels de santé, [...] à l'exception des informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant un tel tiers. » Source : article L1111-7 du Code de Santé publique	• Résultats d'examen • Comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation • Protocoles et prescriptions thérapeutiques mis en œuvre • Feuilles de surveillance • Correspondances entre professionnels de santé	• Les professionnels de santé et du secteur médico-social • Les établissements de santé et du secteur médico-social • Les centres de santé • Le Service de santé des Armées • L'Institution nationale des Invalides

Catégorie	Définition	Exemples	Produites / Collectées par...
Données médico-administratives	« Les données administratives [...] contenues dans les documents médicaux relatifs au traitement d'un patient. » Source : G 29, 5 février 2015, Lettre sur la santé mobile, Annexe, p. 2 ; G 29, Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), 15 févr. 2007, p. 8	• Les informations comme le numéro de sécurité sociale ou la date d'admission à l'hôpital (ou toute autre donnée de traçabilité d'un établissement de santé liée au suivi des patients) • Les données contenues dans le Dossier Pharmaceutique (médicaments délivrés au cours des quatre derniers mois) et le Système national des données de santé (nomenclature et date des actes de soins réalisés, factures, etc.) • Les données produits (version, composition, caractéristiques, contraintes d'utilisation, etc.)	• Les professionnels, établissements et centre de santé et du secteur médico-social, le Service de santé des Armées, l'Institution nationale des Invalides • Les pharmacies • L'Assurance Maladie • Les mutuelles
Données statistiques	Les données statistiques sont des informations codifiées, figées et transmissibles. Elles peuvent être quantitatives comme qualitatives.	• Données agrégées (épidémiologie, etc.)	• Les professionnels, établissements et centre de santé et du secteur médico-social, le Service de santé des Armées, l'Institution nationale des Invalides • L'administration centrale (ex. ministère des Solidarités et de la Santé, ministère de l'Enseignement Supérieur et de la Recherche, Santé publique France) • L'Assurance Maladie • Les mutuelles • Les ARS

Catégorie	Définition	Exemples	Produites / Collectées par...
Données de vie réelle	« Des données qui sont sans intervention sur les modalités usuelles de prise en charge des malades et ne sont pas collectées dans un cadre expérimental (le cadre notamment des essais randomisés contrôlés, ERC), mais qui sont générées à l'occasion des soins réalisés en routine pour un patient, et qui reflètent donc a priori la pratique courante. De telles données peuvent provenir de multiples sources : elles peuvent être extraites des dossiers informatisés de patients, ou constituer un sous-produit des informations utilisées pour le remboursement des soins ; elles peuvent être collectées de manière spécifique, par exemple dans le cadre de procédures de pharmacovigilance, ou pour constituer des registres ou des cohortes, ou plus ponctuellement dans le cadre d'études ad hoc ; elles peuvent également provenir du web, des réseaux sociaux, des objets connectés, etc. » Source : B. Bégaud, D. Polton et Franck von Lennep, « Les données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé : L'exemple du médicament », mai 2017.	• Pression artérielle • Rythme cardiaque • Glycémie • Poids • Informations sur l'état mental et psychologique, sur la qualité du sommeil, sur l'activité physique (ex. nombre de pas), sur le cycle menstruel, le fait d'effectuer plusieurs recherches sur des sujets de santé dans un moteur de recherche	Dans les cas où les données sont récoltées par des dispositifs médicaux (DM) : • Les professionnels de santé et du secteur médico-social • Les citoyens • Les industriels • Les associations et fédérations de patients Dans les cas où les données sont récoltées par des objets connectés, des applications (hors-DM) ou lors des activités en ligne des individus : • Les professionnels de santé et du secteur médico-social • Les citoyens eux-mêmes • Les développeurs d'applications / d'objets connectés et autres acteurs du numérique
Données scientifiques	Données issues de la recherche médicale et des expérimentations scientifiques.	• Registres et cohortes • Résultats d'enquêtes épidémiologiques • Résultats d'études cliniques	• Les médecins-chercheurs • Les pouvoirs publics • Les industriels • Les associations et fédérations de patients
Données contributives	Les données contributives sont des données issues de partages volontaires de la part des citoyens, dans une logique ascendante. Source : Renaissance Numérique & Syntec Numérique (2019), Tous acteurs des données. Appréhender les données pour mieux les valoriser , p.85	• Réponses à des questionnaires • Données partagées dans le cadre d'études cliniques / de programmes de recherche (ex. les données épidémiologiques anonymisées remontées volontairement par certains individus dans le cadre de la lutte contre le Covid-19)	• Les citoyens • Les associations et fédérations de patients • Les chercheurs • Les industriels • Les pouvoirs publics • Les mutuelles

Si la santé est un secteur historiquement riche en données, sa numérisation a démultiplié la quantité de données produites et est venue renforcer la diversité de leurs sources. Non seulement les acteurs de la santé, à l'instar des laboratoires pharmaceutiques, proposent leurs propres dispositifs connectés (systèmes d'autosurveillance de la glycémie, pacemakers), mais de nouveaux acteurs (start-ups, grands groupes du numérique) investissent également de plus en plus le domaine de la santé. Au mois de mars 2019, Apple a ainsi introduit sur le marché français une nouvelle version de sa montre connectée, qui permet à tout utilisateur de réaliser un électrocardiogramme²⁹, examen de l'activité cardiaque habituellement réalisé par les cardiologues. De son côté, Google, par l'intermédiaire de sa filiale X (anciennement Google X Lab), s'est lancé dans le développement de lentilles de contact intelligentes, permettant de détecter le niveau de glucose dans les larmes afin de surveiller le diabète. La firme de Mountain View a également lancé une vaste étude dans le cadre de laquelle les données génétiques et les caractéristiques biochimiques de volontaires en bonne santé sont récoltées, en vue d'identifier les traits qui font défaut chez les individus atteints de pathologies³⁰. On compte, par ailleurs, en France, pas moins de 685 start-ups investies dans le champ de la *healthtech*³¹, et le potentiel du marché de la e-santé dans notre pays est estimé entre 16 et 22 milliards d'euros par an³². Aux données récoltées ou générées via des outils numériques, il faut ajouter celles produites dans le cadre des parcours de soins (les données dites « médicales »), comme par exemple les résultats d'examen, les comptes-rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, les protocoles et prescriptions thérapeutiques mis en œuvre, les feuilles de surveillance ou encore les correspondances entre professionnels de santé. Comme précisé dans le Tableau 1 ci-avant, les données de santé peuvent, en outre, être des données médico-administratives, statistiques, de vie réelle, scientifiques ou même contributives. Elles peuvent aussi bien être recueillies par un professionnel de santé ou du secteur médico-social dans le cadre du

29 Apple, Enregistrement d'un ECG à l'aide de l'app ECG sur l'Apple Watch Series 4, Series 5 ou Series 6 : <https://support.apple.com/fr-fr/HT208955>

30 University of Illinois Chicago, « How Google's « Moonshot » Initiatives Could Change Healthcare » : <https://healthinformatics.uic.edu/blog/how-googles-moonshot-initiatives-could-change-healthcare/>

31 Source : ce chiffre est issu de la base de données dynamique Motherbase : <https://www.motherbase.ai/>, consultée le 4 mars 2021.

32 Institut Montaigne (2020), *E-santé : augmentons la dose !*, 220 pp. : <https://www.institutmontaigne.org/publications/e-sante-augmentons-la-dose>

parcours de soins (par exemple, lors d'une consultation médicale en cabinet ou à l'hôpital) que par une association de patients par le biais d'un questionnaire ou par un industriel via un dispositif médical connecté (DMC). En fonction du contexte dans lequel elles sont utilisées, ces dernières peuvent être nominatives, agrégées, pseudonymisées, anonymisées, etc. Les formes sous lesquelles elles existent sont également extrêmement variées : texte (ex. compte-rendu d'hospitalisation), chiffres (ex. taux de glucose dans le liquide interstitiel), images (ex. radio de la cheville), sons, vidéos. Comme illustré par l'infographie ci-après, elles sont produites, collectées et utilisées dans un ensemble de contextes extrêmement variés.

LE SNDS : UNE BASE DE DONNÉES UNIQUE AU MONDE

Le Système national des données de santé (SNDS), base de données gérée par l'Assurance Maladie, a été créé par la loi de modernisation de notre système de santé du 26 janvier 2016. Il s'agit plus exactement du regroupement de plusieurs bases de données :

le Système national d'information interrégimes de l'Assurance Maladie (SNIIRAM) : un entrepôt de données regroupant les informations issues

- des remboursements effectués par l'ensemble des régimes d'assurance maladie pour les soins du secteur libéral ;
- les données des hôpitaux et autres établissements de santé, issues du Programme de médicalisation des systèmes d'information, le PMSI ;
- la base du CépiDC de l'Institut national de la santé et de la recherche médicale (Inserm), qui rassemble les données sur les causes médicales de décès pour l'ensemble de la population.

Le SNDS constitue ainsi une base de données détaillée sur le parcours des patients et l'organisation du système de soins sur le territoire français.

LES DONNÉES DE SANTÉ : UN ÉCOSYSTÈME HÉTÉROGÈNE



DES DONNÉES SOUVENT CLOISONNÉES ET PEU INTEROPÉRABLES

Du fait de cette grande diversité, à la fois dans leur nature, leur source de production, ou encore leur finalité, les données de santé sont dispersées dans des multitudes de bases de données, qui ne communiquent pas nécessairement entre elles et sont administrées par différents acteurs de la chaîne de santé. Parmi ces dernières, il existe en France une base nationale unique en Europe, voire au monde, le Système national des données de santé (SNDS), qui rassemble des données de santé pseudonymisées, collectées par plusieurs organismes publics. Cette base de données est gérée par l'Assurance Maladie.

Le SNDS fait figure d'exception. La plupart des bases de données de santé existantes en France sont gérées à un niveau très local, par exemple par les cabinets médicaux et les établissements de santé (hôpitaux, EHPAD), qui détiennent toutes les informations afférentes au suivi de leur patientèle. Il existe également des bases de données à des niveaux intermédiaires, comme celles détenues par les associations et communautés de patients, les centres de recherche comme l'Institut national de la santé et de la recherche médicale (Inserm) ou encore les acteurs du secteur privé. L'ensemble des données de santé disponible sur notre territoire obéit ainsi à des logiques et des référentiels de collecte et de restitution souvent différents. **En décou-
lent des données à la qualité, aux référentiels et aux formats extrêmement
variés, ce qui rend difficile leur appariement**³³. Or, c'est précisément sur la possibilité de croiser des données issues de bases différentes, que reposent leur valeur et de nombreuses améliorations (voire innovations) en santé qui peuvent permettre, par exemple, de diagnostiquer des pathologies plus rapidement ou de développer des traitements et dispositifs médicaux plus efficaces. Outre le fait que ces données soient difficilement appariables, il arrive également que ces dernières restent « en silo » et que leur plein potentiel ne soit pas exploité, soit car les acteurs ne disposent pas des ressources nécessaires à leur exploitation, soit car cette dernière n'est pas jugée pertinente. Or, si des médecins-chercheurs au sein d'un hôpital souhaitent par exemple mener une étude sur une maladie rare, il est fort probable que les seules données disponibles dans leur entrepôt de données ne soient pas suffisantes pour aboutir à des conclusions probantes.

33 Rapprochement d'ensembles de données distincts, à l'aide d'informations communes (par exemple, regroupement des données patient issues de différentes sources).

DE LA VALEUR DES DONNÉES

Une donnée prise isolément n'a que peu de valeur. Les données primaires doivent être agrégées et traitées pour qu'il puisse en être dégagé une valeur suffisamment conséquente. Le plus souvent, une donnée n'est d'ailleurs exploitable que lorsqu'elle est contextualisée, utilisée en combinaison avec les métadonnées³⁴ qui l'accompagnent.

Par ailleurs, le simple fait de collecter un nombre important de données ne garantit pas la création de valeur. La valorisation des données est le résultat de mécanismes complexes de collecte, de stockage et de traitement des données destinés à la production de biens ou services à valeur ajoutée.

Un préalable indispensable à toute extraction de valeur à partir des données est la production de données de qualité. De nombreuses données sont en effet rendues inaccessibles ou inutilisables du fait de la mauvaise qualité de leur production. La plupart des données nécessitent donc d'être retraitées avant de pouvoir être utilisées. L'objet de ce traitement est de rendre les données fiables, cohérentes, accessibles pour les utilisateurs et conformes aux normes de sécurité et de confidentialité.

Une fois garantie la qualité des bases de données, leur traitement par des méthodes d'analyse est une étape indispensable de la création de valeur. Par exemple, les traitements algorithmiques permettent la création de services à forte valeur ajoutée, qui apprennent continuellement des données d'usage. La valeur des données n'est donc pas seulement liée à leur abondance et à leur qualité. Leur traitement apparaît tout aussi indispensable à la création de biens et services performants.

Tout au bout de la chaîne, la dernière étape du processus de création de valeur à partir des données tient à leur restitution sous forme de services à destination de l'utilisateur.

Source : Renaissance Numérique & Syntec Numérique (2019), Tous acteurs des données. Appréhender les données pour mieux les valoriser, 97 pp.

34 Les métadonnées désignent l'ensemble des données qui servent à décrire une autre donnée, qu'il s'agisse du nom, de la taille et de la date de création d'un fichier, du titre d'une chanson ou d'un album associés à un fichier audio ou encore du descriptif d'une photographie.

VERS UNE PLATEFORMISATION DES DONNÉES DE SANTÉ

En partie pour ces raisons, on assiste, depuis plusieurs années, à un mouvement de regroupement de certaines bases de données de santé au sein de plateformes numériques. L'objectif de ces initiatives : favoriser un accès sécurisé, simplifié et accéléré aux données de santé, démultiplier la puissance des recherches internes (des hôpitaux et centres de recherche, notamment), mettre en commun des compétences complémentaires (médecins-chercheurs, *data scientists*, statisticiens) et disposer d'une plateforme technologique qui facilite le traitement de données et offre des capacités de calculs et de stockage décuplées. C'est précisément dans cette optique qu'a été lancé au mois de décembre 2020 le *Ouest Data Hub* (voir Tableau 2), première plateforme de données hospitalières en Europe, qui vise, à terme, le regroupement des données de six centres hospitaliers³⁵ au service de la recherche médicale. Le groupement des Hôpitaux Universitaires du Grand Ouest (HUGO), qui gère cette plateforme, collabore également avec d'autres réseaux de CHU en vue de développer ce modèle original de « hub interrégional ». Au niveau national, cet élan est incarné par le lancement, en 2020 également, de la plateforme des données de santé, le *Health Data Hub* (voir encadré p. 43-44). Comme exposé dans le Tableau 2 ci-après, ces différentes plateformes de données de santé ont chacune leur logique propre et visent à répondre à des objectifs différents (recherche, enjeux organisationnels, soins, coordination, etc.). Les plateformes privées spécialisées, par exemple, répondent à une offre de soins, à un besoin de santé. Elles ont donc une vocation différente des plateformes rassemblant des bases de données destinées à des travaux de recherche à l'instar du *Health Data Hub* ou de celles gérées par l'Inserm.

TABLEAU 2 - LA PLATEFORMISATION DES DONNÉES DE SANTÉ

Plateformes publiques nationales	 Accessible aux acteurs publics comme privés à des fins de recherche, d'étude ou d'évaluation
Plateformes publiques inter-régionales	 Accessible uniquement aux chercheurs du groupement des Hôpitaux Universitaires du Grand Ouest (HUGO)
	 Accessible aux professionnels de santé, aux chercheurs, aux cadres administratifs des hôpitaux, et éventuellement aux industriels
Plateformes publiques transfrontalières/européennes	 Accessible dans un premier temps à l'ensemble des professionnels de santé des États membres
Plateformes privées spécialisées	 Accessible aux patients diabétiques équipés d'appareils de mesure en continu du glucose FreeStyleLibre et aux professionnels de santé qui les suivent
	 Accessible aux cliniciens pour le suivi quotidien de leurs patients (rassemble des données disponibles en temps réel, comme les paramètres vitaux, la pression artérielle et le poids des patients)

Parmi les différentes échelles de mise en commun de données de santé via des plateformes numériques, il ne faut pas oublier l'échelon européen. Dans sa stratégie pour les données publiée en février 2020³⁷, la Commission européenne a, en effet, posé les bases d'un « espace européen commun des données relatives à la santé ». L'objectif : renforcer et étendre l'utilisation et la réutilisation des données de santé au niveau de l'UE. Le *Health Data Hub* est d'ailleurs l'autorité compétente pour la France dans le cadre de l'action conjointe lancée par la Commission européenne pour définir les contours

36 Voir : <https://www.philips.fr/healthcare/innovation/a-propos-de-healthsuite/applications>

37 Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité Économique et Social européen et au Comité des Régions, « Une stratégie européenne pour les données », COM(2020) 66 final, 19 février 2020, 41 pp.

35 Les CHU d'Anger, Brest, Nantes, Rennes et Tour, et le CHR d'Orléans.

de cet espace commun de données³⁸. Une proposition législative est attendue à cet égard pour fin 2021/début 2022. Enfin, comme souligné dans le Tableau 2, certaines données de santé sont mises à disposition au sein de plateformes développées par des acteurs privés. C'est le cas, par exemple, des données liées au suivi des patients diabétiques équipés de dispositifs de mesure en continu du glucose de type « FreeStyle Libre », qui sont accessibles aux patients et leurs médecins via la plateforme LibreView. Bien qu'obéissant à des logiques et objectifs variés, les diverses plateformes de données de santé existantes n'opèrent pas nécessairement en silo les unes par rapport aux autres. Elles font partie d'un écosystème au sein duquel on observe de plus en plus de coordination. Certaines plateformes développées par des acteurs du secteur numérique peuvent notamment faire l'objet de partenariats avec des industriels du secteur de la santé, voire être intégrées au catalogue de services référencés par la puissance publique via l'Espace numérique de santé (ENS) baptisé « Mon Espace Santé », l'espace personnel où les citoyens français pourront accéder à des services et gérer leurs données de santé à partir du premier janvier 2022 (voir encadré p. 73). Alors que les initiatives de rassemblement et de mise à disposition de données de santé via des plateformes numériques se multiplient à divers échelons, la question de leur articulation devient de plus en plus prégnante, ce qui rend d'autant plus complexe la lisibilité et la gouvernance de ces données.

« On essaie d'avoir une étape de gouvernance intermédiaire, au sein de l'Inserm, notamment sur les cohortes. Les CHU font de même avec les entrepôts de données. Ensuite, il faudra organiser le dialogue entre le Health Data Hub et ces structures de gouvernance intermédiaires. »

Franck Lethimonnier,

DIRECTEUR DE L'INSTITUT THÉMATIQUE « TECHNOLOGIES POUR LA SANTÉ » À L'INSERM

Le relatif cloisonnement des données de santé, qui freine leur exploitation, y est pour beaucoup dans cette dynamique actuelle de « plateformes ». Il explique également les efforts consentis récemment par le gouvernement dans le cadre de la stratégie nationale « Ma Santé 2022 » et du plan France Relance. Ces derniers visent notamment à moderniser la flotte des équipements informatiques (logiciels, systèmes d'information) des professionnels et des établissements de santé, et à favoriser l'adoption de référentiels d'interopérabilité et de sécurité socles. L'objectif : décroiser les données de santé pour encourager leur utilisation. Toutefois, si de grands chantiers sont lancés, la gouvernance des données de santé reste pour l'heure encore peu lisible.

...À UNE GOUVERNANCE PEU LISIBLE DE CES DONNÉES

UN PILOTAGE DE LA POLITIQUE PUBLIQUE DES DONNÉES DE SANTÉ RELATIVEMENT FLOU

Tout questionnement afférent au pilotage de la politique publique des données de santé doit nécessairement s'inscrire dans un cadre plus large, qui dépasse ces seules données : celui du « numérique en santé » et des enjeux qui le sous-tendent et, de façon générale, celui de la transformation numérique de l'action publique. En France, plusieurs entités, notamment le ministère des Solidarités et de la Santé, le secrétariat d'État chargé du Numérique, l'Agence du numérique en Santé (ANS), la Caisse nationale de l'Assurance Maladie (CNAMTS) ou encore Santé publique France, se partagent les commandes de la gouvernance de la politique du numérique en santé. Au sein même du ministère de la santé, plusieurs services sont très impliqués, notamment la Délégation ministérielle du numérique en santé (DNS), chargée de mettre en place la feuille de route stratégique du numérique en santé, la Direction générale de l'offre de soins (DGOS), responsable, entre autres, du programme Expérimentations de télémédecine pour l'amélioration des parcours en santé (ETAPES)³⁹, et la Direction de la recherche, des études, de

38 Pour en savoir plus, voir : <https://www.health-data-hub.fr/actualites/kick-officiel-de-laction-conjointe-espace-europeen-des-donnees-de-sante>

39 Un programme national qui, depuis 2018, encourage et soutient financièrement le déploiement de projets de télésurveillance sur l'ensemble du territoire, et ce par le biais d'expérimentations autour de cinq pathologies : l'insuffisance cardiaque, l'insuffisance rénale, l'insuffisance respiratoire, le diabète et les prothèses cardiaques implantables.

l'évaluation et des statistiques (DREES)⁴⁰. Bien appréhender le pilotage de la politique publique des données de santé nécessite de comprendre le rôle de chacune de ces entités dans la gouvernance du numérique en santé, ce qui n'est pas toujours aisé, y compris pour des initiés. Dans son rapport *Confiance, innovation, solidarité : Pour une vision française du numérique en santé*⁴¹ paru en juin 2020, le Conseil national du numérique (CNNum) évoquait l'exemple du développement de l'Espace numérique de santé (ENS). Alors que le pilotage stratégique de ce chantier a été confié à la Délégation ministérielle du numérique en santé, c'est la Caisse nationale de l'Assurance Maladie qui en assure le pilotage opérationnel, tandis que l'Agence du numérique en santé définit le cadre d'interopérabilité et que la DGOS intervient sur les leviers financiers⁴². Bien que cette gouvernance partagée puisse être compréhensible (chaque acteur exerce bien là une compétence pour laquelle il dispose d'une expertise reconnue), cette multiplicité d'acteurs peut participer du manque de lisibilité et d'agilité des chaînes de décision et mener à une certaine lenteur d'exécution, voire à des situations de blocage.

Tous, en effet, n'ont pas nécessairement la même perception et la même utilisation des données de santé. Comme observé dans le cadre de la lutte contre l'épidémie de Covid-19, il est arrivé, par exemple, qu'en analysant un même jeu de données, Santé publique France et la DREES ne parviennent pas aux mêmes chiffres pour certaines variables. La raison ? Les données en question n'étaient pas redressées (ou pré-traitées) de la même façon par les deux entités qui, au final, ne parlaient pas exactement le même langage.

Ce point apparaît d'autant plus critique qu'il semblerait que certaines des organisations impliquées dans le pilotage du numérique en santé ne possèdent pas pleinement les moyens nécessaires à la mise en œuvre des missions qui leur sont confiées. À l'occasion des auditions menées dans le cadre de ce rapport, il a notamment été souligné que la Délégation ministérielle du numérique en santé ne serait pas suffisamment fournie en personnel compte tenu de la feuille de route fixée.

Cette relative faiblesse tient également au fait qu'on est ici à la frontière de

deux mondes : celui de la santé et celui du numérique. Gouverner (au sens politique du terme) le « numérique en santé » ou la « santé numérique » nécessite que ces deux mondes se coordonnent en vue d'établir une stratégie claire et cohérente. Lors des échanges que le think tank a pu avoir avec les acteurs du système de santé, plusieurs d'entre eux ont dénoncé un problème de portage politique, notamment (mais pas uniquement) autour du *Health Data Hub*, qui selon eux devrait être porté par le ministre des Solidarités et de la Santé. Il y a là également des enjeux de lisibilité pour les citoyens et de confiance de ces derniers vis-à-vis des pouvoirs publics. Des points d'autant plus critiques lorsqu'il s'agit de la santé publique. Si, sur des questions aussi importantes que le *Health Data Hub* ou les applications de traçage des cas de Covid-19, les citoyens français assistent à un débat désordonné, cela ne participe ni de leur confiance en ces dispositifs ni de leur bonne compréhension de ces enjeux. À ce titre, on peut regretter que les débats autour de l'application StopCovid aient quasi-exclusivement été concentrés sur des enjeux de sécurité des données et de souveraineté numérique (que la grande majorité des citoyens ne maîtrisent pas), laissant de côté les problématiques liées à la santé. La crise a révélé les difficultés qui demeurent à débattre collectivement, à la fois concernant des enjeux techniques et de santé publique, les citoyens étant par ailleurs majoritairement exclus de ces débats. Afin d'embarquer l'ensemble des acteurs dans la transformation numérique du secteur de la santé, il apparaît donc nécessaire de définir un pilotage plus clair de la politique publique des données de santé.

UN ÉCOSYSTÈME DIFFICILE À APPRÉHENDER DANS SA GLOBALITÉ

Le partage et l'utilisation des données dans le secteur de la santé offrent de nombreuses opportunités de développement économique et social, au bénéfice des citoyens et des professionnels de santé, comme des entreprises ou de l'État. Toutefois, appréhender l'écosystème des données de santé dans sa globalité n'est pas chose aisée.

DONNÉES DE SANTÉ, DONNÉES MÉDICALES, DONNÉES DE BIEN-ÊTRE : DES NOTIONS POREUSES

Depuis plusieurs années, start-ups et grandes entreprises du numérique ont largement investi le champ de la santé. Ainsi, l'écosystème des données de santé rassemble à la fois des acteurs de la chaîne de santé, à l'instar des labo-

40 Fabrice Lenglard, Directeur de la DREES, a par ailleurs été récemment nommé administrateur des données du ministère des Solidarités et de la Santé.

41 Conseil national du numérique (2020), *Confiance, innovation, solidarité : Pour une vision française du numérique en santé*, 114 pp. : <https://cnnumerique.fr/files/uploads/2020/ra-sante-cn-num-web.pdf>

42 Ibid., p. 37.

ratoires pharmaceutiques, des mutuelles et assurances, ou des pouvoirs publics, mais également des acteurs du secteur numérique. Inévitablement, cette arrivée de nouveaux entrants a entraîné une complexification de l'écosystème des données de santé, au sein duquel les frontières entre des notions comme « données médicales » et « données de bien-être » sont relativement poreuses. Si tous les objets connectés et autres applications numériques utilisés dans le cadre des parcours de soins ne sont pas nécessairement considérés comme des dispositifs connectés (DM) récoltant des données médicales, certains ont été certifiés par la *Food and Drug Administration* (FDA) américaine⁴³ et sont en passe de devenir des DM. Qui plus est, la qualification d'une donnée comme « donnée médicale » ou « donnée de bien-être » peut être amenée à changer au cours de la vie de ladite donnée, une donnée de bien-être pouvant très bien devenir une donnée médicale.

Si nombre de ces nouveaux acteurs développent des solutions reposant sur le traitement algorithmique de données, certains fabricants d'objets connectés commercialisent des produits dont certaines fonctionnalités les placent à la frontière entre les dispositifs médicaux connectés (DMC) et les objets connectés (ex. les bracelets Fitbit, l'iWatch d'Apple). Or, les exigences réglementaires afférentes à la commercialisation de ces solutions ne sont pas les mêmes. En l'occurrence, celles concernant la mise sur le marché de dispositifs médicaux (DM) sont plus strictes. Les entreprises qui développent des DMC sont, en effet, tenues de respecter un cadre légal relativement rigoureux (marquage CE, développement d'études cliniques, validation des autorités de santé préalable à la mise sur le marché). Ces obligations ne sont pas applicables aux objets connectés qui ne sont pas considérés comme des dispositifs médicaux (quand bien même ces derniers permettent d'analyser certains aspects de l'état de santé d'une personne). Ces derniers ne font, de ce fait, pas non plus l'objet d'un remboursement par la sécurité sociale. Ils sont toutefois soumis à d'autres réglementations existantes, par exemple en matière de protection des données personnelles (ex. RGPD).

De fait, la frontière entre la nature des données recueillies par des DMC (données médicales) et celle des données issues d'objets connectés (données « de bien-être » ou « de bonne santé ») s'estompe. Cela soulève inévitablement des questions quant au cadre légal entourant ces technologies, notamment en

termes de responsabilité. L'usage d'objets connectés, s'il n'est pas encadré du point de vue sanitaire, pourrait par exemple conduire les citoyens à prendre des décisions sur leur santé en se fondant sur les mesures que leur renvoient ces appareils. Puisqu'ils permettent de mesurer des aspects de l'état de santé d'une personne, ces outils ne devraient-ils pas alors faire l'objet de contrôles plus stricts lors de leur mise sur le marché ? *A minima*, une vigilance accrue sur l'impact de ces derniers est souhaitable. Des réflexions émergent à ce sujet. Lors de nos échanges avec les parties prenantes, certains ont, par exemple, proposé l'instauration d'une sorte de référentiel pour ces dispositifs, qui garantisse *a minima* leur fiabilité, une version allégée des référentiels imposés aux industriels des dispositifs médicaux connectés (normes ISO, référentiels d'interopérabilité et de sécurité, etc.). D'autres, au contraire, sont contre cette idée et sont d'avis que le marché opérera automatiquement une sélection des solutions les plus fiables. La logique voudrait que cela dépende de l'intention des fabricants de ces outils. Si ces derniers visent une incorporation de leurs solutions dans des parcours de soins ouvrant droit à un remboursement avec des fonds publics (cf. via l'Assurance Maladie), alors il est nécessaire que le législateur puisse fixer les conditions de cette prise en charge, et un « référentiel allégé » semblerait judicieux. S'ils entendent, en revanche, limiter la commercialisation de leurs outils au marché privé, alors ce serait plutôt aux assureurs (ex. les mutuelles) d'arbitrer cela. Il est en tout état de cause primordial que, dans le cadre de la commercialisation de leurs innovations en santé, les acteurs issus du secteur numérique prennent en compte ces aspects.

La question se pose également de l'éventuelle utilisation de ces données, récoltées par toute une série d'objets connectés (bracelets, montres, balances, etc.) au bénéfice du système de santé, par exemple dans le cadre des parcours de soins ou de la recherche médicale. Certaines données dites de « bien-être » (qualité du sommeil, activité physique, calories assimilées, etc.) pourraient être mobilisées par les professionnels de santé afin d'étayer leurs diagnostics. Ces objets n'étant pas soumis aux mêmes exigences de précision que les dispositifs médicaux, une telle démarche nécessiterait toutefois de s'interroger sur la fiabilité des données en question. Une étude publiée dans le *Journal of Clinical Sleep and Medicine* en novembre 2019 a par exemple démontré que les dispositifs portables (*wearables*, en anglais) Fitbit de suivi du sommeil, montrent une sensibilité acceptable mais une faible spécificité, ce qui leur confère une précision encore insuffisante pour pouvoir être utilisés dans

⁴³ La *Food and Drug Administration* est l'autorité de régulation américaine des denrées alimentaires et des médicaments. Elle a, entre autres, le mandat d'autoriser la commercialisation des médicaments sur le territoire des États-Unis.

des environnements cliniques⁴⁴. La même année, une étude publiée dans la revue *Annals of Translational Medicine*, qui portait sur l'efficacité de plusieurs montres intelligentes dans la détection de la fibrillation auriculaire⁴⁵, a abouti à des conclusions similaires⁴⁶. Ses auteurs ont notamment précisé que si ces technologies ne sauraient constituer l'outil ultime de diagnostic dudit trouble, elles peuvent tout de même servir de dispositifs d'alerte, incitant leurs utilisateurs à consulter un médecin pour avoir une confirmation dans le cas où une irrégularité du rythme cardiaque serait détectée. De son côté, une étude parue dans le *Journal of Strength and Conditioning Research* a conclu que le dispositif BioHarness développé par le groupe Zephyr, ainsi que le bracelet Fitbit Charge, démontrent d'excellentes mesures de fiabilité. Selon les auteurs de l'étude, des mesures stables et cohérentes de la fréquence cardiaque et de l'activité physique peuvent être obtenues à l'aide de ces dispositifs⁴⁷. Ces résultats laissent à penser qu'il existe des limites à l'utilisation des données récoltées par les objets connectés à des fins médicales, et que des recherches supplémentaires dans ce domaine sont nécessaires au cas par cas.

Les récents travaux du Laboratoire d'Innovation Numérique de la CNIL (LINC) ont par ailleurs montré comment des informations concernant la santé des individus peuvent être inférées à partir de « *traces numériques anodines (comportement en ligne, clic, utilisation des réseaux sociaux, etc.) et sans aucun lien direct avec un état de santé* »⁴⁸. Le professeur et chercheur en droit américain Mason Marks utilise le terme de « données émergentes de santé » pour faire référence à ces traces numériques *a priori* anodines, mais qui permettent un profilage des utilisateurs de services numériques – parfois à des fins commerciales – en fonction de leur état de santé.

44 Moreno-Pino, F., Porras-Segovia, A., López-Esteban, P., Artés, A., et Baca-García, E., « Validation of Fitbit Charge 2 and Fitbit Alta HR Against Polysomnography for Assessing Sleep in Adults With Obstructive Sleep Apnea », *Journal of Clinical Sleep Medicine*, Volume 15, Issue 11, 15 novembre 2019, pp. 1545-1653 : <https://jcs.m.aasm.org/doi/full/10.5664/jcs.m.8032>

45 Un trouble du rythme cardiaque.

46 Raja, JM., Elsagr, C., Roman, S., Cave, B., Pour-Ghaz, I., Nanda, A., Maturana, M., et Khouzam, RN., « Apple Watch, Wearables, and Heart Rhythm: where do we stand? », *Annals of Translational Medicine*, Volume 7, Issue 17, septembre 2019 : <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6787392/>

47 Nazari, G., MacDermid, JC., Sinden, KE., Richardson, J., et Tang, A., « Reliability of Zephyr BioHarness and Fitbit Charge measures of heart rate and activity at rest, during the modified Canadian Aerobic Fitness Test, and recovery », *Journal of Strength and Conditioning Research*, Volume 33, Issue 2, février 2019, pp. 559-571 : https://journals.lww.com/nsca-jscr/Abstract/2019/02000/Reliability_of_Zephyr_Bioharness_and_Fitbit_Charge.32.aspx

48 Biéri, M., « Les données sociales sont des données de santé comme les autres », Laboratoire d'Innovation Numérique de la CNIL, 17 mai 2021 : <https://linc.cnil.fr/les-donnees-sociales-sont-des-donnees-de-sante-comme-les-autres>

De fait, la frontière entre ce qui constitue une donnée de santé et ce qui n'en est pas une est relativement poreuse. En outre, l'écosystème des données de santé évolue extrêmement rapidement. En résulte une difficulté à l'appréhender dans sa globalité.

DES LOGIQUES DE COLLECTE ET DE GESTION PEU HARMONISÉES RESTREIGNENT L'INTEROPÉRABILITÉ ET LE PARTAGE DES DONNÉES DE SANTÉ

La complexité de l'écosystème des données de santé relève également d'enjeux techniques, notamment en termes d'interopérabilité. Malgré des principes généraux d'encadrement qui s'appliquent à tous les acteurs impliqués dans la collecte de données de santé, il existe des variations dans l'application de ce dernier. Ainsi, au fil du temps, ces acteurs ont développé leurs propres procédures de recueil et de gestion des données, et défini leurs propres règles d'accès à leurs bases de données (lorsque celles-ci sont accessibles). Ainsi, au niveau local, certains grands centres hospitaliers possèdent leurs propres « entrepôts » de données⁴⁹, dont ils gèrent le fonctionnement et les accès. C'est par exemple le cas de l'Assistance publique-Hôpitaux de Paris (AP-HP), qui a mis en place un entrepôt rassemblant des données concernant 11 millions de patients⁵⁰. Au sein même de l'AP-HP, un Comité scientifique et éthique est chargé d'analyser les demandes et d'accorder les accès aux données de l'entrepôt. Les centres hospitaliers universitaires (CHU) de Nantes et de Lille possèdent des entrepôts de données de santé (EDS) similaires. Sans aller jusqu'à établir un EDS, chaque établissement de santé possède en général, *a minima*, son propre système d'information permettant à son personnel de stocker et consulter les données afférentes au suivi des patients et au fonctionnement de l'établissement. De même, certains centres de recherche possèdent et gèrent leurs propres bases de données destinées à la recherche médicale. C'est le cas de l'Institut national de la santé et de la recherche médicale (Inserm), qui est promoteur ou responsable de l'organisation de plus de 70 cohortes⁵¹ en France. Bien qu'elles représentent un patrimoine exceptionnel, ces milliards de données obéissent souvent à des

49 Un entrepôt de données de santé est un « système d'information commun, qui vise à faciliter la réalisation de recherches dans le domaine de la santé et d'études relatives au pilotage hospitalier en regroupant dans une base unique l'ensemble des données recueillies dans les établissements ». Houdart & Associés, « Les entrepôts hospitaliers de données : du mythe à la réalité », 12 novembre 2019 : <https://www.houdart.org/les-entrepots-hospitaliers-de-donnees-du-mythe-a-la-realite/>

50 AP-HP, « Comprendre les données de l'EDS » : <https://eds.aphp.fr/nos-services/eds-donnees>

51 Voir : <https://www.inserm.fr/recherche-inserm/recherche-en-sante-publique/cohortes>

standards différents ne sont, de fait, pas interopérables⁵². Cela limite grandement leur partage entre les différents acteurs de l'écosystème.

UNE EXPLOITATION ÉGALEMENT LIMITÉE PAR LES LOGIQUES DE THÉSAURISATION DE CERTAINS ACTEURS

La faiblesse de circulation n'est pas due uniquement à leur manque d'interopérabilité. À cet obstacle d'ordre technique, s'ajoute la problématique de la propriété des bases de données. Si les données récoltées peuvent être, à l'origine, des données personnelles, la plupart des institutions impliquées dans la collecte de données de santé, qu'il s'agisse par exemple d'établissements de santé ou d'instituts de recherche, estiment que les bases constituées par leurs soins sont leur propriété. Selon Stéphanie Combes, Directrice du *Health Data Hub*, des questions comme « *le partage de la valeur créée et de la propriété intellectuelle liées à la mise à disposition de ces données* » sont sources de blocages. « *Certains CHU ou centres de recherche veulent que chaque société privée qui va accéder aux données contractualise avec eux et se mette d'accord sur un partage de la valeur créée.* »⁵³ Car ils dépensent énormément de moyens et de temps au recueil de ces données, il arrive également que certains acteurs soient tentés de se réserver l'exclusivité de leur exploitation et refusent de les mettre en commun. Ainsi, le potentiel de ces dernières n'est pas exploité au-delà du contexte et des études pour lesquels elles ont été collectées, alors même que c'est précisément le croisement de diverses données qui permet de révéler toute leur valeur.

En mars 2018, le « rapport Villani » préconisait, dans une section dédiée à l'intelligence artificielle au service des politiques de santé, la création d'une plateforme nationale « *d'accès et de mutualisation des données pertinentes pour la recherche et l'innovation en santé* »⁵⁴. C'est l'ambition du *Health Data Hub*, la plateforme nationale des données de santé lancée au printemps 2020, qui s'est fixé pour objectifs de donner accès aux données de santé, soutenir la collecte et la consolidation de ces données, accompagner leur valorisation et leur analyse, et

soutenir l'écosystème et assurer le lien avec la société civile.⁵⁵ Face aux logiques de thésaurisation des données adoptées par certains acteurs du système de santé, la démarche du *Health Data Hub* est claire : faire du partage la règle, de la fermeture l'exception. La mission de préfiguration de la plateforme précisait, à ce titre, que « *les données financées par la solidarité nationale doivent être partagées avec tous les acteurs, publics comme privés, et bénéficier ainsi au système de santé, à la recherche, au tissu industriel et à l'assurance du maintien de la souveraineté nationale sur un secteur stratégique* »⁵⁶.

UN AN APRÈS SON LANCEMENT, OÙ EN EST LE HEALTH DATA HUB ?

Créé par la loi du 24 juillet 2019 relative à l'organisation et la transformation du système de santé, le *Health Data Hub* (HDH) a officiellement débuté ses activités de façon anticipée au mois d'avril 2020, afin de permettre le croisement de données afférentes au Covid-19. Son organisation prend la forme d'un groupement d'intérêt public (GIP), associant 56 parties prenantes, dont la Haute Autorité de Santé (HAS), France Assos Santé, l'Assurance Maladie, le CNRS, l'AP-HP, les CHU de Toulouse et Limoges et le Conseil national de l'ordre des médecins⁵⁷.

Toute personne ou structure, publique ou privée, peut faire une demande d'accès aux données mises en commun au sein du *Health Data Hub* en vue de réaliser une étude, une recherche ou une évaluation présentant un intérêt public. La pertinence (en particulier leur caractère d'intérêt public) des projets soumis est analysée par le Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES), qui rassemble des experts scientifiques, éthiques, juridiques, et des représentants des associations de patients. La CNIL se prononce ensuite sur l'autorisation ou non du projet. Pour l'heure, 26⁵⁸ projets sont accompagnés au sein de la plateforme⁵⁹.

52 L'interopérabilité est la capacité d'un système informatique à communiquer, exécuter des programmes ou transférer des données avec d'autres produits ou systèmes informatiques, existants ou futurs, sans contrainte pour l'utilisateur dans l'accès ou la mise en œuvre, et sans multiplier les efforts de développements. Source : <https://www.houdart.org/les-entrepots-hospitaliers-de-donnees-du-mythe-a-la-realite/>

53 « Les données de santé, un trésor mondialement convoité », *Le Monde*, 2 mars 2020 : https://www.lemonde.fr/sciences/article/2020/03/02/les-donnees-de-sante-un-tresor-mondialement-convoite_6031572_1650684.html

54 Cédric Villani, *Donner un sens à l'intelligence artificielle - Pour une stratégie nationale et européenne*, mars 2018, p. 201 : https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf

55 *Health Data Hub*, Mission de préfiguration, octobre 2018, p. 32 : https://solidarites-sante.gouv.fr/IMG/pdf/181012_-_rapport_health_data_hub.pdf

56 Ibid., p. 19.

57 Pour la liste complète, voir l'arrêté du 29 novembre 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé » : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039433105>

58 Au 17 mars 2021.

59 Pour la liste complète, voir : <https://www.health-data-hub.fr/partenariats>

Si le catalogue des données⁶⁰ disponibles au sein du HDH se limite au moment de la rédaction de ce rapport à la base « Organisation de la surveillance coordonnée des urgences » (OSCOUR) gérée par Santé publique France et aux données issues du SNDS concernant les patients avec un diagnostic hospitalier de Covid-19, ce dernier prévoit d'accueillir, entre autres, une collection de bases de données issues du SNDS, le registre France Greffe de Moelle⁶¹, la cohorte I-share⁶² et la base des 500 000 angioplasties⁶³. Il convient de noter ici que l'objectif n'est pas de rassembler, au sein d'une base ou d'une plateforme unique, cet ensemble de données. Au lieu de cela, les bases de données concernées sont répliquées puis enrichies au sein du HDH. L'enrichissement du catalogue des bases de données disponibles est la priorité des équipes du *Health Data Hub* pour l'année 2021.

Plusieurs grands chantiers en cours, à l'instar de la mise en place du *Health Data Hub*, ou du développement de référentiels nationaux en matière de sécurité et d'interopérabilité, devraient ainsi permettre de décloisonner les données et de favoriser leur partage et leur réutilisation.

DES DONNÉES DONT LA SENSIBILITÉ ACCENTUE LA COMPLEXITÉ

Au-delà des caractéristiques évoquées jusque-là, c'est également la haute sensibilité des données de santé qui rend particulièrement complexe leur appréhension par les différents acteurs de la chaîne de santé. Ces données sont, en effet, des données extrêmement intimes susceptibles, qui plus est, d'être utilisées à mauvais escient. Leur partage et leur exploitation soulève dès lors de forts enjeux d'ordre éthique, mais également d'ordre technique, notamment en matière de confidentialité et de sécurité.

60 Voir : <https://www.health-data-hub.fr/catalogue-de-donnees>

61 Le registre national des donneurs volontaires de moelle osseuse.

62 La cohorte I-share constitue la plus grande étude scientifique jamais réalisée sur la santé des jeunes, qui rassemble plus de 20 000 volontaires qui répondent à des questions sur 12 sujets liés à leur santé, comme le sommeil, le stress ou encore l'alimentation.

63 Des données qui permettent d'étudier l'impact des *stents* (endoprothèses vasculaires) dans la vie réelle.

DE LA SENSIBILITÉ DES DONNÉES DE SANTÉ

LA CONFIDENTIALITÉ, UN ENJEU AU CŒUR DE L'EXPLOITATION DES DONNÉES DE SANTÉ

Car elles concernent l'intimité des personnes, la confidentialité des données de santé est un enjeu clé. À cet égard, elles sont protégées par le droit au respect de la vie privée⁶⁴, qui s'incarne notamment par le secret médical.

LE SECRET MÉDICAL : UN REMPART HISTORIQUE CONTRE LA DIVULGATION DE DONNÉES À CARACTÈRE PERSONNEL CONCERNANT LA SANTÉ

En France, le secret médical est consacré par un ensemble conséquent de textes juridiques, dont :

- le Code de la santé publique
- le Code de la sécurité sociale
- le Code civil
- le Code pénal
- le Code général des collectivités territoriales
- le Code du sport
- le Code de l'action sociale et des familles
- la Loi Informatique et Libertés
- l'arrêt du Conseil d'État du 26 septembre 2018 relatif à l'étendue du secret médical (identité des patients)

Conformément à l'article L1110-4 du Code de la santé publique, « toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent

64 Voir, sur le site [vie-publique.fr](https://www.vie-publique.fr), la fiche thématique « Chaque citoyen a-t-il droit au respect de sa vie privée ? » : <https://www.vie-publique.fr/fiches/23879-chaque-citoyen-t-il-droit-au-respect-de-sa-vie-privee>

code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant. »

La violation du secret médical peut donner lieu à des sanctions professionnelles, civiles et pénales allant jusqu'à un an d'emprisonnement et 15 000 euros d'amende⁶⁵.

Afin d'assurer la continuité des soins, les professionnels d'une même « équipe de soins » peuvent, toutefois, être amenés à échanger des informations médicales nécessaires au suivi médico-social d'un patient⁶⁶. Depuis 2016, la loi définit ainsi la notion de « secret partagé » (article L1110-4 du Code de la santé publique) et en précise les limites. La définition de l'équipe de soins est quant à elle énoncée à l'article L1110-12 du Code de la santé publique. Il convient de noter ici que le cadre légal n'est pas le même dans tous les États membres de l'Union européenne, et que la définition de l'équipe de soins varie notamment d'un pays à l'autre. Une dimension qui aura son importance dans la matérialisation de l'ambition d'une gouvernance européenne des données de santé.

Du fait des préjudices (discriminations, risques d'exclusion sociale) que la révélation de données personnelles concernant la santé pourrait entraîner, la réglementation applicable à la protection de ces dernières entraîne une obligation systématique d'information du patient pour toute collecte, ainsi que la nécessité du consentement pour l'exploitation de ses données médicales.

Il est en outre important que ces données soient maintenues secrètes vis-à-vis de certains acteurs en particulier : par exemple, les assurances et les employeurs ou potentiels employeurs. Parmi les risques associés au partage et à l'exploitation des données de santé, plusieurs des acteurs interrogés dans le cadre de ce rapport ont évoqué le « risque assurantiel », soit le fait pour des compagnies d'assurance de proposer des offres opérant une distinction dans le montant des primes en fonction des risques identifiés par analyse des données de santé des individus. Afin de prévenir ce risque, la loi interdit tout traitement du Système

65 Article 226-13 du Code pénal.

66 Jusqu'à 2016, il n'était pas possible pour un médecin d'échanger, par exemple, avec un psychologue, à propos d'un patient commun. Désormais, avec la notion de « secret partagé », cela est possible, au sein d'une même équipe de soins.

national des données de santé (SNDS) qui viserait à l'exclusion de garanties des contrats d'assurance ou à la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque.

Il convient de relever également que toutes les données à caractère personnel concernant la santé, qui forment un ensemble très hétérogène, ne revêtent pas le même niveau de sensibilité. Certaines, comme les données génétiques, sont extrêmement sensibles du fait de leur dimension « pluripersonnelle ». Il en va ainsi de notre ADN, qui contient une partie de l'ADN des membres de notre famille. Cette particularité rend la question du consentement en cas du traitement de ces données particulièrement difficile. Alors que le traitement de données génétiques est interdit en France, se sont développées, ces dernières années, un certain nombre d'offres basées sur des tests génétiques. La plateforme en ligne MyHeritage propose, par exemple, un test ADN qui promet à ses utilisateurs de « *trouver de nouveaux membres de leurs familles et [...] découvrir leur origines ethniques* »⁶⁷. Un développement d'autant plus problématique qu'en cas de fuite de données issues de tests ADN, les caractéristiques physiologiques et psychologiques d'un individu peuvent potentiellement être identifiées et exploitées par des cybercriminels afin de mener des attaques informatiques très ciblées, de type ingénierie sociale et hameçonnage.^{68 69} La Commission nationale de l'informatique et des libertés (CNIL), très sollicitée sur le sujet, surveille ces développements de près.

DE CET IMPÉRATIF DE CONFIDENTIALITÉ DÉCOULE UN IMPÉRATIF DE PROTECTION ET DE SÉCURITÉ

En raison du fort impératif de confidentialité qui surplombe les données de santé, ces dernières comportent inévitablement un important enjeu de protection et de sécurité. Un autre risque qui a été souvent cité par les acteurs interrogés dans le cadre de ce rapport, est le **risque d'intrusion dans des systèmes d'information hébergeant des données de santé, à des fins malveillantes**.

67 Voir : <https://www.myheritage.fr/dna>

68 Sur ce sujet, voir les travaux de Renaud Lifchitz, spécialiste de la cybersécurité, notamment sa présentation « DIY DNA OSINT! or... how to enhance your social engineering skills using recent genomics » lors du Forum International de la Cybersécurité 2019 : <https://speakerdeck.com/rlifchitz/diy-dna-osint-or-dot-dot-dot-how-to-enhance-your-social-engineering-skills-using-recent-genomics>

69 « Les tests ADN en kit, une nouvelle mine d'or pour les pirates ? », Interview de Renaud Lifchitz, spécialiste de la cybersécurité, *BFM Business*, 28 janvier 2020 : https://www.bfmtv.com/tech/vie-numerique/les-tests-adn-en-kit-une-nouvelle-mine-d-or-pour-les-pirates_AN-202001280085.html

De fait, ce risque est une réalité de tous les jours. Les cyberattaques à l'encontre d'établissements de santé et laboratoires d'analyses médicales tendent à se multiplier de par le monde, y compris en France. Ainsi, au mois de février 2021, le Centre hospitalier de Dax et l'Hôpital Nord-Ouest de Villefranche-sur-Saône ont été victimes d'attaques par rançongiciel⁷⁰. Mais si ces exemples ont marqué l'actualité, ils ne représentent que la partie émergée de l'iceberg. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) recense environ une tentative d'attaque par semaine sur des infrastructures comme les EHPAD, les CHU, les hôpitaux et les cliniques ou autres entités en lien avec des services de santé⁷¹. En février 2020, Renaissance Numérique alertait sur la nécessité de l'ensemble du système de santé de monter en maturité sur les enjeux de cybersécurité, la diffusion rapide des outils et des usages numériques en son sein accroissant *de facto* la surface d'exposition aux cyber risques⁷². L'accélération de la stratégie nationale en matière de cybersécurité présentée par Emmanuel Macron le 18 février 2021 vise en partie à répondre à ces enjeux. Ainsi, « *pour chaque programme numérique, les structures de santé seront invitées à consacrer systématiquement 5 à 10 % du budget à la cybersécurité, notamment au maintien en condition de sécurité des SI dans la durée.* »⁷³ À la suite de ces annonces, un appel à manifestation d'intérêt a en outre été lancé, afin d'expérimenter des solutions innovantes destinées à répondre aux besoins en matière de cybersécurité de trois types de structures, dont les établissements de santé⁷⁴.

Le plus souvent, la finalité des cyberattaques à l'encontre des établissements de santé est de paralyser les opérations des structures victimes en attendant le paiement d'une rançon. Leur objet n'est donc pas systématiquement de dérober les données de santé détenues par les établissements afin

d'en faire un usage détourné, même si cela est de plus en plus souvent le cas. En témoigne le récent détournement d'une base de données personnelles concernant la santé de près de 500 000 citoyens français, qui a été vendue sur des espaces de discussion spécialisés dans l'achat et la vente de fichiers piratés, puis diffusée en accès libre sur des forums de discussion⁷⁵. Dans ce cas précis, les données dérobées étaient issues des fichiers de 28 laboratoires différents, qui utilisaient tous un logiciel qui n'était plus mis à jour par son éditeur.^{76 77} Si cet exemple souligne l'importance à accorder à la sécurisation des données de santé d'un point de vue technique, il pose également la question de la responsabilité des structures qui récoltent et gèrent des données de santé. Par ailleurs, selon l'ANSSI, le phénomène dit de la « double extorsion » est aujourd'hui de plus en plus répandu. Dans ce cas de figure, les attaquants exfiltrent les données, en publient une partie pour faire pression sur l'établissement victime et, quand bien même ce dernier accepte de payer la rançon demandée, mettent en vente les données sur des forums cybercriminels⁷⁸.

Au-delà des menaces externes, le risque en matière de sécurité des données peut provenir d'erreurs humaines de la part des personnes ayant accès à ces données, ces deux dimensions n'étant pas excluant. C'est le cas notamment lorsque des procédures de sécurité ne sont pas respectées. Comme souligné lors d'un entretien par Jacques Lucas, président de l'Agence du numérique en santé, les intrusions dans un système d'information sont souvent liées au non-respect (même involontaire) des procédures de sécurité établies pour accéder et ressortir dudit système d'information. A également été évoquée dans le cadre de ces auditions une pratique vraisemblablement répandue au sein du corps hospitalier, qui consiste à s'échanger des données de santé (des comptes-rendus, de l'imagerie médicale) via des messageries qui ne sont pas suffisamment sécurisées pour échanger des données de santé (WhatsApp, Messenger), les outils de téléexpertise disponibles étant peu ergonomiques, complexes et non disponibles sur smartphones. S'il peut y avoir des failles de

⁷⁰ Selon l'Agence nationale de sécurité des systèmes d'information (ANSSI), un rançongiciel ou *ransomware* est une technique d'attaque courante de la cybercriminalité qui consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

⁷¹ « Pourquoi les cyberattaques contre les hôpitaux ne vont pas s'arrêter », *L'Usine Nouvelle*, 16 février 2021 : <https://www.usinenouvelle.com/article/pourquoi-les-cyberattaques-contre-les-hopitaux-ne-vont-pas-s-arreter.N1061559>

⁷² Renaissance Numérique (2020), *Cybersécurité : Accompagner un système de santé en pleine mutation*. Accessible en ligne : https://www.renaissancenumerique.org/system/attach_files/files/000/000/217/original/NOTE_CYBERSANTE.pdf?1582567842

⁷³ « Accélération de la stratégie nationale en matière de cybersécurité », Élysée, 18 février 2021 : <https://www.elysee.fr/emmanuel-macron/2021/02/18/strategie-nationale-cybersecurite>

⁷⁴ « Cybersécurité à l'hôpital : lancement d'un appel à manifestation d'intérêt pour expérimenter des solutions innovantes », *Tic Santé*, 30 mars 2021 : <https://www.ticsante.com/story/5622/cybersecurite-a-l-hopital-lancement-d-un-appel-a-manifestation-d-interet-pour-experimenter-des-solutions-innovantes.html>

⁷⁵ « Cinq questions sur la fuite des données médicales de 500 000 Français sur le Web », *Le Monde*, 25 février 2021 : https://www.lemonde.fr/pixels/article/2021/02/25/cinq-questions-sur-la-fuite-des-donnees-medicales-de-500-000-francais-sur-le-web_6071223_4408996.html

⁷⁶ *Ibid.*

⁷⁷ Dedalus, Communiqué de presse, 26 février 2021 : https://www.dedalus-france.fr/wp-content/uploads/2021/02/21.02.26_CP-Dedalus-France-confirme-investiguer-sur-un-grave-acte-de-cybercriminalite-C3%A9-et-a-identifi%C3%A9-et-pr%C3%A9venu-les-laboratoires-concern%C3%A9s.pdf

⁷⁸ ANSSI, Centre gouvernemental de veille et d'alerte et de réponse aux attaques informatiques, « État de la menace rançongiciel à l'encontre des entreprises et institutions », 1 mars 2021, p. 13 : <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf>

sécurité technologiques, les failles humaines sont donc également largement répandues. Cet enjeu de sécurité entraîne des contraintes technico-légales fortes en termes d'accès aux données de santé et de modalités de traitement. La capacité des acteurs concernés à assurer et prendre en charge financièrement toute faille de sécurité pèse en outre particulièrement fort sur les plus petits d'entre eux (start-ups, hôpitaux de petite taille).

L'EXPLOITATION DES DONNÉES DE SANTÉ REVÊT DES DIMENSIONS ÉTHIQUES QUI DOIVENT FAIRE L'OBJET D'UNE ATTENTION PARTICULIÈRE

Si le partage et le traitement des données de santé sont strictement encadrés du point de vue de la sécurité, c'est également car ils revêtent de fortes dimensions éthiques, qui vont au-delà des enjeux de confidentialité déjà évoqués. Comme le souligne le Comité consultatif national d'éthique (CCNE) pour les sciences de la vie et de la santé dans son avis 130, le principal enjeu en la matière est de « *trouver le bon équilibre entre le risque d'une sous-exploitation des données limitant des recherches menées dans l'intérêt général et celui d'un partage des données trop large et insuffisamment contrôlé mettant en cause les droits fondamentaux de la personne.* »⁷⁹

À titre d'exemple, il convient de s'interroger sur le cadre applicable à la commercialisation de ces données. En France, les données personnelles de santé sont soumises à un régime spécifique semblable à celui dont relève le corps humain. Conformément au Code civil et à la jurisprudence applicable, les données personnelles des individus ne sont en effet pas considérées comme des propriétés, mais comme un droit attaché à la personne humaine. À ce titre, elles ne peuvent ni être cédées, ni être vendues (en dehors des exceptions et conditions prévues par la loi). Cette position rejoint les mêmes considérations éthiques ayant poussé les législateurs à interdire le traitement des données issues du SNDS visant la différenciation des primes d'assurances en fonction des risques. Mais qu'en est-il des données dites de « bien-être » recueillies par des applications ou par le biais d'objets connectés tels que les bracelets, les montres et les balances, qui donnent des indications sur l'état de santé des individus ? Le programme Vitality de l'assureur Generali propose, par exemple, aux salariés qui le souhaitent de synchroniser avec sa plateforme leurs objets connectés et autres applications de suivi d'activité physique, et de recevoir en échange des récompenses (chèques cadeau, bons de réduction) à dépenser

chez ses partenaires. Si le régime standard du RGPD s'applique dans ce cas de figure (les données en question n'étant pas considérées comme des données de santé), cette pratique, et notamment le fait que l'entreprise considère que ces données ne sont pas des données de santé, peut poser question. Cette qualification des données ainsi collectées a-t-elle été soumise à l'analyse du régulateur ? Quand bien même il serait admis qu'il s'agit de données de bien-être et non pas de données de santé, le fait qu'elles soient collectées par un employeur sur ses employés (vis-à-vis desquels il existe un rapport de subordination, rendant ces derniers potentiellement plus vulnérables), ne devrait-il pas entraîner un niveau de sensibilité supérieur des données collectées ? Au-delà de leur nature, l'identité du responsable de traitement peut générer un niveau de sensibilité supérieur aux données collectées.

De la même façon, il convient de s'assurer que le recours à des outils basés sur l'exploitation de données de santé n'entraîne pas une inégalité d'accès aux soins. En effet, alors que le manque de littératie numérique persiste au sein de la société, la numérisation de la santé ravive à certains égards ce risque. Ainsi, au mois de février, les centres de vaccination contre le Covid-19 du département de Seine-Saint-Denis ont vu affluer des patients des départements voisins, plus connectés et habitués à prendre des rendez-vous sur des plateformes comme Doctolib. Résultat : parmi les bénéficiaires du vaccin accueillis au centre municipal de santé de La Courneuve les quinze premiers jours, seulement 20 % étaient Courneuviens. Comment s'assurer, dès lors, que la numérisation du secteur de la santé ne se fasse pas au détriment des plus démunis ? Comment garantir l'égal accès aux soins des personnes qui ne peuvent pas ou qui ne souhaitent tout simplement pas utiliser ces outils ? Cette question mérite d'être mise au cœur des débats visant à définir le système de santé de demain.

Enfin, la possibilité de mettre en place des traitements massifs de données (*big data*) dans le secteur de la santé, par exemple pour entraîner des algorithmes d'aide au diagnostic, suscite également des interrogations, notamment en matière de prédiction. Plus exactement, il s'agit de définir jusqu'où la médecine prédictive peut aller sans contrevenir aux droits fondamentaux des individus. Si demain, grâce à un algorithme, il est possible de prédire qu'un individu a 96 % de chances de mourir d'un cancer des poumons avant ses 50 ans, que devra-t-on faire de cette information ? Convendra-t-il de la transmettre à l'individu en question, et le cas échéant, à quel moment de sa vie ? Cette question n'est pas nouvelle et se pose depuis longtemps à propos de la détection de maladies génétiques. Dans ce cadre-là, le choix est laissé

⁷⁹ Comité consultatif national d'éthique pour les sciences de la vie et de la santé (2019), *Données massives et santé : Une nouvelle approche des enjeux éthiques*, Avis 130, p. 8 : <https://www.ouvrir-lascience.fr/donnees-massives-et-sante-une-nouvelle-approche-des-enjeux-ethiques/>

aux personnes concernées de savoir ou de ne pas savoir si elles sont porteuses du gène incriminé. Une même logique pourrait alors être appliquée vis-à-vis des prédictions algorithmiques, et l'on peut, par exemple, imaginer qu'un professionnel de santé demande à son patient « Souhaitez-vous savoir ou non ce que l'algorithme a prédit ? ». Quelle que soit la solution retenue, celle-ci relève d'un choix de société quant à notre vision commune du système de santé. Avancer dans la voie du partage et de l'exploitation des données de santé nécessite d'appréhender ces questions collectivement.

UN CADRE LÉGAL STRICT, QUI AGIT EN GARDIEN

Du fait des enjeux éthiques et techniques qui les entourent, les données de santé font l'objet d'un encadrement légal strict. Au niveau européen, elles sont considérées comme une catégorie particulière de données personnelles au sens du Règlement général sur la protection des données (RGPD), au même titre que les données portant sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale. Conformément à l'article 9(1) du RGPD, **leur traitement est donc en principe interdit**. Il existe cependant un certain nombre d'exceptions à ce principe d'interdiction, listées au paragraphe 9(2) du règlement. S'agissant des données de santé, plusieurs exceptions sont susceptibles de s'appliquer, notamment :

- lorsque le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale ;
- lorsque la personne concernée a donné son consentement explicite ;
- lorsque le traitement est nécessaire à la sauvegarde d'intérêts vitaux ;
- lorsque le traitement est nécessaire pour des motifs d'intérêt public importants ;

- lorsque le traitement est nécessaire à des fins de recherche scientifique⁸⁰.

En France, la loi Informatique et Libertés leur reconnaît également un niveau de sensibilité particulier et consacre l'interdiction de leur traitement (article 6). Comme le RGPD, elle énonce toutefois des exceptions, qui constituent les conditions dans lesquelles les données de santé peuvent être communiquées et utilisées : suivi médical, diagnostics, soins, prévention, recherche médicale, élaboration de statistiques dans le domaine de la santé, évaluation ou analyse des pratiques de santé, etc.⁸¹.

Ce cadre légal, qui est donc à la fois européen et propre à chaque pays (la santé demeurant une prérogative des États membres de l'Union européenne), entraîne un certain nombre d'obligations technico-légales concernant l'accès aux données de santé, leur traitement et leur hébergement, que les responsables de traitement doivent respecter. La procédure d'accès aux données dépend, en outre, de la nature de la recherche, de l'organisme réalisant la demande, ainsi que des données auxquelles il souhaite accéder. Comme cela a été souligné, certains entrepôts de données de santé (EDS) détenus par des centres hospitaliers possèdent leurs propres règles d'accès, parfois administrées par un comité scientifique et éthique. En l'absence d'harmonisation des règles d'accès aux données entre acteurs de la santé, il faut donc se référer, pour chaque base visée, aux instructions de demande d'accès spécifiques à la structure qui met les données à disposition. Le schéma 2 ci-après détaille par exemple le parcours permettant d'accéder aux données de l'EDS de l'AP-HP.

⁸⁰ En France, celle-ci est pour l'instant limitée à la recherche revêtant un intérêt public. Ainsi, les organisations privées souhaitant accéder aux données mises à dispositions au sein du *Health Data Hub* doivent prouver au Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES) le caractère d'intérêt public que présente leur projet de recherche.

⁸¹ Voir : Titre II, Chapitre III, Section 3 - Traitements de données à caractère personnel dans le domaine de la santé, de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Kit de demande CSE :
<https://recherche.aphp.fr/eds/recherche>

Si partenaires externes

Après autorisation par le CSE, les méthodologistes GH préparent la requête de l'étude

Processus de demande (bleu) :

- Demande de recherche multicentrique
- Rédaction projet
- Comité scientifique et éthique
- Contrat DRCI
- Sélection de patients

Processus de recherche (vert) :

- Paramétrage
- Création de l'espace de travail
- Alimentation
- Installation des logiciels tiers
- Accès aux données
- Analyse de données sur la plateforme mégadonnées AP-HP

ÉQUIPE RECHERCHE (jupyter)

Central (EDS AP-HP, PACS AP-HP)

Espace privé Cluster EDS Hadoop

Serveurs AP-HP

***Méthodologiste :** coordinateur + référents (DIM, URC, Santé publique) + Data scientists du GH

Source : eds.aphp.fr/nos-services/recherche-innovation

Si on prend l'exemple des données du Système national des données de santé (SNDS), il faut distinguer deux types d'accès :

- un accès permanent, au bénéfice de certains services ou organismes publics (Direction générale de la santé, agences régionales de santé, Agence nationale de sécurité du médicament et des produits de santé (ANSM), etc.) pour l'accomplissement de leurs missions et dans des limites fixées par décret^{B2} ;
- un accès ponctuel, soumis à l'accomplissement préalable d'une formalité vis-à-vis de la Commission nationale de l'informatique et des libertés, pour les autres organismes (structures privées, par exemple), pour certaines finalités fixées par le Code de la santé publique, telles que la réalisation d'une étude, d'une recherche ou d'une évaluation et répondant à un motif d'intérêt public^{B3}.

Tout organisme désirant obtenir un accès ponctuel aux données du SNDS doit remplir une formalité auprès de la CNIL. Deux procédures sont possibles : soit l'organisme déclare que l'objet de sa demande est conforme à une des méthodologies de référence développées par l'autorité⁸⁴, soit (en cas de non-conformité) il dépose auprès de cette dernière une demande d'autorisation. Des formalités qu'il peut être difficile de mettre en œuvre.

À titre d'exemple, l'accès aux données du SNDS est très encadré pour les entreprises qui fabriquent des produits de santé et pour les assureurs. Ces organismes doivent soit passer par un bureau d'étude ou un laboratoire de recherche indépendant qui traitera les données pour leur compte et leur transmettra des résultats agrégés, soit démontrer que les modalités techniques d'accès ne lui permettent pas d'utiliser les données du SNDS pour des finalités interdites. À l'occasion d'un webinaire sur les données de santé, la recherche et le Covid-19 organisé le 27 janvier 2021, Manon de Fallois, juriste au

82 Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

83 Voir : <https://www.health-data-hub.fr/interet-public>

84 Pour la liste des méthodologies de référence en santé élaborées par la CNIL, voir : https://www.cnil.fr/fr/traitements-declaration-conformite?field_norme_numerotation_type_value%5B0%5D=6

service de la santé de la CNIL, a toutefois expliqué que cette démonstration n'était « *pas nécessairement évidente* » et que « *dans la quasi-totalité des cas, les industriels de santé ou les assureurs préfèrent passer par un laboratoire de recherche ou un bureau d'étude* ».

« Le RGPD, qui est un bon règlement européen pour les citoyens, pose problème depuis un an et demi dans le travail des chercheurs, dans la transposition qui en est faite par les États. Les dossiers que nous portons sur de grands essais cliniques sont instruits par des juristes très pointus sur environ 9-10 mois pour savoir quoi déclarer à la CNIL. L'analyse des risques est très complexe, et on a beaucoup d'interlocuteurs, de documents à remplir. Quand on réfléchit « données de santé » et comment en tirer profit au sein d'un collectif dans une logique de soins, on est confronté à une très grande complexité. »

Franck Lethimonnier,

DIRECTEUR DE L'INSTITUT THÉMATIQUE « TECHNOLOGIES POUR LA SANTÉ » À L'INSERM

Enfin, afin de garantir une protection suffisante des données en question, ces dernières ne doivent pas mentionner les noms des personnes, ni toute autre information qui permettrait directement ou indirectement de les identifier : elles doivent être « pseudonymisées ». La pseudonymisation est un traitement (réversible) de données à caractère personnel qui permet de rendre impossible toute identification de la personne concernée sans avoir recours à des informations supplémentaires, pourvu que ces informations supplémentaires soient conservées séparément et soumises à des mesures de protection⁸⁵. En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, date de naissance, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.). Outre la pseudonymisation, il existe un autre moyen de traiter des données de santé sans porter atteinte à la vie privée des personnes :

l'anonymisation. L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière, cette fois, irréversible. Toutes les informations directement ou indirectement identifiantes sont supprimées ou modifiées. Dans ce cas, la législation relative à la protection des données ne s'applique plus, car la diffusion ou la réutilisation des données anonymisées n'a pas d'impact sur la vie privée des personnes concernées. Toutefois, dans le domaine de la santé, une anonymisation stricte peut rendre certains projets de recherche quasiment irréalisables. Lorsqu'on anonymise une information, on la désindividualise de telle manière qu'aucune possibilité de ré-individualiser une caractéristique n'est possible, par toute déduction ou par tout croisement. À un tel niveau, faire de la recherche devient compliqué. On ne peut plus, par exemple, établir de cohortes de personnes qui se ressemblent, car elles n'ont plus de caractéristiques qui les singularisent. Certaines données, à l'instar des données génomiques, sont par ailleurs impossible à anonymiser totalement.

Au vu de la sensibilité qui caractérise les données de santé, l'existence d'un cadre légal protecteur des individus et de leurs données est indispensable. Si le cadre actuel définit une protection au niveau de l'individu, peut-être serait-il envisageable, sur certains sujets, que la protection soit pensée au niveau de l'intérêt collectif plutôt qu'au niveau de l'intérêt individuel des personnes dont les données sont traitées.

PROTECTION INDIVIDUELLE VS. SANTÉ PUBLIQUE ?

Basé essentiellement sur la protection des données personnelles, le cadre légal entourant les traitements de données de santé place l'individu au centre des préoccupations. Ce constat peut être considéré comme évident, dans la mesure où ces données sont des données « individualisantes ». Toutefois, l'immense quantité de données produites par le système de santé et la capacité de les exploiter de façon sécurisée ouvre de nouvelles perspectives en matière de santé publique (épidémiologie, organisation des soins, etc.). À l'heure actuelle, tout est fait pour que les citoyens, à titre individuel, soient protégés contre une éventuelle atteinte à leur vie privée. Cette démarche est bien entendu nécessaire et louable. Poussée à l'extrême, elle peut néanmoins faire obstacle à l'accomplissement de certains objectifs collectifs de santé publique.

⁸⁵ Voir à cet égard l'article 4(5) du RGPD et le point 6.1. de l'annexe à l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé.

Procéder à un traitement de données de santé nécessite de s'inscrire dans l'une des exceptions mentionnées par le RGPD. À cet égard, il ressort des auditions menées dans le cadre de ce rapport que la base légale la plus souvent retenue serait celle du consentement des personnes dont les données font l'objet d'un traitement (article 9(2)(a)). En plus d'être informé du traitement de ses données et de la finalité dudit traitement, l'individu doit donner son consentement libre, spécifique, éclairé et univoque⁸⁶. Par exemple, lors de la conception de l'application de suivi des cas contact StopCovid (devenue depuis TousAntiCovid), la CNIL, comme l'autorité allemande de protection des données⁸⁷, a décidé de requérir le consentement des individus. Indépendamment des questions que cela peut poser au regard des objectifs de santé publique, le consentement comporte des limites, y compris du point de vue de la protection individuelle. **La difficulté que pose le consentement est qu'il doit être libre et éclairé, ce qui n'est pas systématiquement le cas.** Hélène Guimiot-Bréaud, responsable du service de la santé à la CNIL, estime ainsi que « *le respect de l'obligation d'information n'est pas toujours aisé : les informations transmises aux individus peuvent être insuffisantes ou, au contraire, être trop détaillées et prêter à confusion* »⁸⁸. Or, pour que le consentement soit absolument éclairé, il faut une information irréprochable. Qui plus est, dans le domaine de la santé, les personnes qui doivent donner un consentement au traitement de leurs données se trouvent très souvent dans une posture de vulnérabilité. De fait, le consentement n'est, dans de nombreux cas, pas plus libre qu'il n'est éclairé. Dès lors, il ne saurait être la garantie d'une conformité au RGPD et de la bonne protection des individus et de leurs données.

Sans doute est-ce pourquoi les textes ont justement prévu la possibilité de ne pas solliciter le consentement des individus lorsqu'il s'agit de remplir un impératif de santé publique. Malgré cette possibilité, l'arbitrage entre protection des données individuelles et objectifs de santé publique reste difficile. Les régulateurs européens ont tous une vision différente sur le sujet, et la CNIL, comme le montre sa décision d'imposer le consentement pour le déploiement de l'application StopCovid, se montre particulièrement prudente.

86 Considérant (32) du RGPD : « Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant ».

87 Voir la politique de confidentialité de l'application allemande officielle CoronaWarn-App : <https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf>. D'autres régulateurs, par exemple au Royaume-Uni, ont fait le choix de privilégier l'intérêt public. Voir à cet égard la politique de confidentialité de l'application développée par la NHS : <https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice>

88 Audition réalisée par visioconférence le 16 novembre 2020.

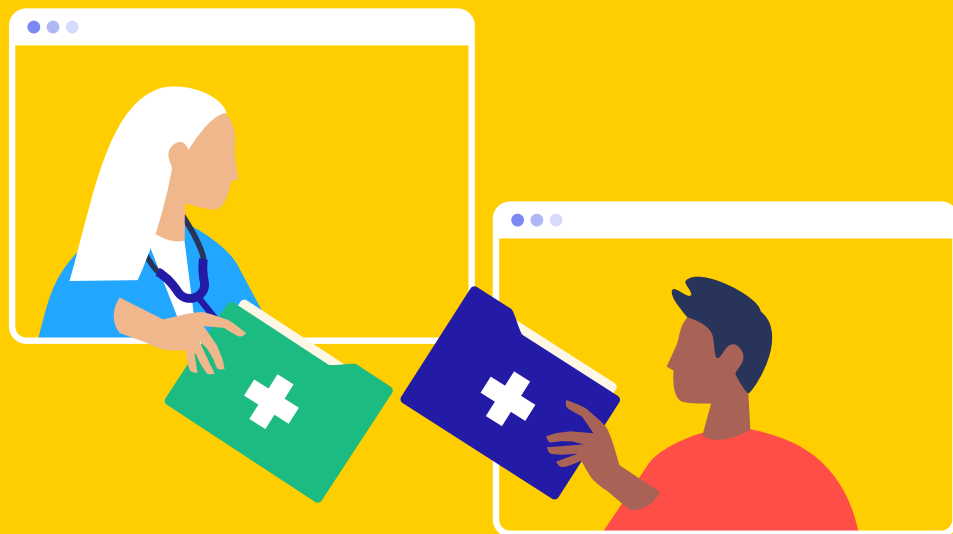
Alors que le RGPD le permet (au nom de l'intérêt public) et que la lutte contre la pandémie de Covid-19 offrait des arguments en faveur de la protection de la santé publique, l'autorité a estimé que cela n'était pas suffisant pour se passer du consentement.

Ces questions relèvent d'arbitrages qui ne dépendent pas d'un seul régulateur, et il y a là une opportunité de redéfinir la démocratie sanitaire, en invitant les différents acteurs de la chaîne sanitaire, jusqu'aux citoyens, à prendre part au débat.

La transformation de notre système de santé par les données numériques est désormais bien enclenchée. Celle-ci soulève toutefois des questions d'ordre éthique, technique et juridique, que l'on doit considérer collectivement. Dans le cadre de l'exploitation de ces données, comment concilie-t-on l'enjeu de protection des libertés individuelles et les objectifs de santé publique ? Jusqu'où doit-on aller en matière de médecine prédictive ? Quel doit-être le rôle des différents acteurs de la chaîne de santé dans la gouvernance de ces données ? Comment garantir l'égal accès aux soins des personnes qui ne peuvent pas ou qui ne souhaitent tout simplement pas utiliser les outils de santé numérique ? Autant de questions qui doivent faire l'objet d'arbitrages, incluant toutes les parties prenantes, jusqu'aux citoyens. Redéfinir la démocratie sanitaire à l'aune des données de santé nécessite toutefois dans un premier temps que tous les acteurs de la chaîne soient mis en capacité de comprendre ce que sont ces données et les problématiques qui sous-tendent leur partage et leur exploitation. Comme présenté dans cette partie, l'écosystème des données de santé est en effet extrêmement riche et complexe, en constante et rapide évolution. Afin que l'ensemble des acteurs de la chaîne de santé, et en particulier les citoyens, puissent se saisir des enjeux qui y sont liés, de sérieux efforts d'« appropriation » sont indispensables.

PARTIE 2

POUR UNE CULTURE DES DONNÉES DE SANTÉ PARTAGÉE



Faire des données un des leviers de la démocratie sanitaire pose un défi d'acculturation massive. Le manque de littératie numérique parmi la population, de même que la complexité propre à l'écosystème des données de santé, limitent, de fait, l'appréhension de ces données. S'il est déjà difficile de comprendre ce qu'est une donnée ou un algorithme, comment s'attendre à ce que tout un chacun comprenne aisément les enjeux que le partage et l'exploitation des données de santé sous-tendent ? Comme l'ont révélé les auditions réalisées dans le cadre de ce rapport, les différents acteurs du secteur de la santé en sont bien conscients, et certains d'entre eux (notamment les mutuelles, la Croix-Rouge, le *Health Data Hub*, l'Assurance Maladie, l'ANS et les ARS) lancent des initiatives en vue de familiariser les citoyens avec la notion de données de santé. En outre, les efforts d'assimilation qu'il convient de réaliser ne concernent pas uniquement la familiarisation des acteurs du monde de la santé (citoyens, patients, professionnels et établissements de santé, mutuelles, Assurance Maladie, industriels, agences régionales et nationales, etc.) à la numérisation de ce secteur. Il convient également de faire monter en capacité les « nouveaux entrants » issus du monde numérique qui investissent le champ de la santé, et qui ne sont pas toujours sensibilisés aux problématiques de cet environnement.

ACCULTURER LES ACTEURS DU SECTEUR DE LA SANTÉ AUX DONNÉES NUMÉRIQUES

Les initiatives gouvernementales visant à numériser le secteur de la santé se poursuivent et ont connu un coup d'accélérateur significatif ces deux dernières années. Malgré cela, on constate une relative méconnaissance de ces dernières de la part des citoyens, ainsi que des usages mitigés de la part des professionnels et établissements de santé. Il ressort toutefois des divers travaux menés par le think tank, de même que des échanges organisés dans le cadre de ce rapport, que ce défaut d'acculturation ne concerne pas uniquement les données de santé, mais plutôt les données (et le numérique) en général. C'est donc toute une culture des données qui est à créer.

« Le manque de littératie numérique est un réel problème. Les gens ne sont pas conscients de leurs droits numériques et ne comprennent pas pleinement que leurs données ont beaucoup de valeur. »

Jelena Malinina,
DIGITAL HEALTH POLICY OFFICER, BEUC

Dans cet effort d'acculturation aux données, la particularité des données de santé ne doit toutefois pas être ignorée. Alors que les citoyens développent progressivement leur connaissance de la valeur de certaines de leurs données, par exemple leurs données bancaires, cette évolution semble pour l'heure exclure les données de santé. Les citoyens ont généralement une méconnaissance à la fois de la définition et de la valeur de leurs données de santé.

LES DONNÉES NUMÉRIQUES DE SANTÉ, DES ACTIFS ENCORE MAL CONNUS

Pour les non-initiés (et même parfois pour les initiés), qualifier le bénéfice des données n'est pas évident. En comparaison au bénéfice que peut produire l'analyse de données de santé, celui apporté par un médicament est, par exemple, relativement simple à appréhender. Si l'on simplifie les choses à l'extrême : on est malade, on prend un médicament, on guérit. Le bénéfice est facile à comprendre car il se vit. À l'inverse, comprendre que le partage et le traitement de données peuvent améliorer la santé est complexe. Cela nécessite de comprendre qu'au cœur du processus, il y a tout un écosystème, qui comporte notamment des chercheurs, des porteurs de projets, qui permettent des innovations, et ainsi de suite. C'est tout l'enjeu du développement de la littératie des données (de l'anglais *data literacy*) ou culture des données, qui se définit comme la capacité à produire, à comprendre et à utiliser les données numériques⁸⁹. À cet égard, 54% des sondés dans le cadre d'un sondage OpinionWay réalisé pour le

89 Renaissance Numérique et Syntec Numérique (2019), *Tous acteurs des données. Appréhender les données pour mieux les valoriser*, p. 81 : <https://www.renaissancenumerique.org/publications/tous-acteurs-des-donnees-apprehender-les-donnees-pour-mieux-les-valoriser>

compte du Ministère des Solidarités et de la Santé en novembre 2020 mentionnent l'exclusion des usagers qui ne sont pas familiers avec le numérique comme principal facteur de risque posé par la création d'un Espace numérique de santé. Les résultats de l'indice européen relatif à l'économie et à la société numériques (DESI) de 2020 montrent, par ailleurs, que seuls 57% de la population française possèdent des compétences numériques élémentaires, un chiffre qui n'a pas évolué depuis 2018⁹⁰. Les personnes ayant des compétences numériques plus avancées ne représentent, elles, que 31% de la population⁹¹.

Mais cette difficile appréhension des données ne relève pas uniquement d'un sujet de littératie. Il s'agit également d'une question d'équipement. Comme révélé dans le dernier baromètre du numérique réalisé par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), le Conseil général de l'économie (CGE)⁹² et la Mission Société Numérique, 12 % de la population française âgée de 12 ans et plus n'est toujours pas connectée à internet⁹³. En outre, une récente étude du think tank Terra Nova a montré que, bien qu'elle se réduise, la fracture numérique persiste entre les territoires, les zones rurales et périphériques demeurant sous-équipées en comparaison aux grandes agglomérations⁹⁴. Embarquer l'ensemble des citoyens dans la transformation numérique de la santé constitue sans aucun doute un des plus grands défis qui attend le secteur dans les années à venir. Faire l'impasse sur cette réalité reviendrait à prendre le risque de mettre en place des outils au niveau national (par exemple, Mon Espace Santé) qui ne seraient utilisés que par une part définie de la population, tandis que d'autres seraient laissés pour compte. Face à ce constat, la nécessité de maintenir des alternatives non-numériques s'impose.

Mettre les citoyens en capacité de « se saisir » de leurs données personnelles de santé est d'autant plus crucial que cette maîtrise est une composante clé de leur capacité à s'impliquer dans les débats afférents à leur utilisation, dont ils sont souvent écartés.

90 Indice relatif à l'économie et à la société numériques (DESI) 2020 - France, p. 9 : <https://digital-strategy.ec.europa.eu/en/policies/desi-france>

91 Ibid.

92 Conseil général de l'économie.

93 ARCEP, CGE, Mission Société Numérique (2019), *Baromètre du numérique 2019 - Enquête sur la diffusion des technologies de l'information et de la communication dans la société française en 2019*, p. 9 : <https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffres/numerique/le-barometre-du-numerique.html>

94 Terra Nova, « Baromètre des résultats de l'action publique : La France de la fibre optique », 16 avril 2021 : <https://tnova.fr/notes/barometre-des-resultats-de-l-action-publique-la-france-de-la-fibre-optique>

Les auditions menées par le think tank dans le cadre de cette étude ont, par ailleurs, révélé **une grande hétérogénéité dans la maturité des professionnels de santé, des associations de patients et des décideurs publics et politiques vis-à-vis des données de santé**. À titre d'exemple, contrairement à certaines entités, les grands CHU possèdent généralement une Direction de l'information médicale (ou équivalent), au sein de laquelle évoluent des spécialistes des données qui travaillent en lien étroit avec les responsables des systèmes d'information. Ces moyens humains leur confèrent des compétences et une maturité particulièrement poussées en matière de données de santé. À l'inverse, d'autres acteurs, comme certaines ARS, possèdent des capacités relativement limitées dans ce domaine. Ces dernières se sont d'ailleurs retrouvées en difficulté durant la crise du Covid-19, lorsqu'elles ont dû mettre en place le traçage des cas contacts puis de la vaccination, sans que des ressources supplémentaires ne leur soient allouées. D'une ARS à l'autre, il arrive également que les compétences en matière de traitement de données varient grandement, notamment en fonction des moyens consacrés aux directions de la statistique.

Y compris au sein de l'administration centrale, notamment dans les différents ministères, la sensibilisation des agents à ces questions reste pour l'heure relativement limitée. Le plan de transformation de l'action publique présenté par la ministre Amélie de Montchalin au mois de mars 2021⁹⁵ et nourri par les travaux de la « mission Bothorel », vise à pallier ce déficit. Il est en effet prévu que, d'ici au mois de septembre 2021, chaque ministère complète une feuille de route précisant les contours de la gouvernance de ses données, ainsi que les politiques d'ouverture et de valorisation des données qu'ils auront mises en place. Une demande également appuyée via une circulaire signée par le Premier ministre Jean Castex et adressée aux membres du gouvernement et aux préfets de région, à qui il rappelle : « *Il vous appartient également de mettre en place l'organisation la plus adaptée pour favoriser les synergies entre les services chargés du numérique dans votre ministère, notamment les services statistiques. À cette fin, vous nommerez d'ici le 15 mai un administrateur ministériel des données, chargé d'élaborer la stratégie de votre ministère dans ce domaine, de coordonner les parties prenantes et d'être le point de contact des utilisateurs des données et des applica-*

tions numériques relevant de votre périmètre. »⁹⁶. Une personne référente a ainsi été désignée dans chaque ministère⁹⁷. Pour le ministère des Solidarités et de la Santé, il s'agit de Fabrice Lenglard, Directeur de la DREES. Le plan de modernisation de la fonction publique comprend également un volet visant à ouvrir davantage les données afin de piloter les politiques publiques de manière plus efficace et permettre une plus grande transparence de l'action publique. Cette ambition témoigne d'une prise de conscience de l'importance de se saisir de la problématique des données au plus haut niveau de l'État. Tout l'enjeu est maintenant de diffuser effectivement cette culture des données dans les différentes branches de l'administration de la santé.

FAVORISER L'ACCULTURATION DE TOUS AUX DONNÉES DE SANTÉ

DÉVELOPPER UNE SENSIBILISATION GÉNÉRALE AUX DONNÉES DE SANTÉ À TOUS LES TEMPS DE LA VIE

Pour une maîtrise partagée des données de santé, **il convient de penser à un continuum d'éducation, qui ne se rapporte pas uniquement à une éducation à la culture des données**. Ce dernier doit être organisé autour de trois axes : une éducation à la citoyenneté numérique au sens large, une éducation sanitaire et une éducation thérapeutique.

AGIR SUR TROIS AXES D'ACCULTURATION AUX DONNÉES DE SANTÉ DES CITOYENS

Renaissance Numérique identifie trois axes prioritaires d'éducation pour installer une « culture des données de santé » chez les citoyens :

95 Ministère de la Transformation et de la Fonction Publiques, « 400 jours pour accélérer la transformation numérique de l'État », Dossier de presse, 4 mars 2021 : <https://www.transformation.gouv.fr/files/presse/Dossier-de-presse-400-jours-accelerer-transformation-numerique-etat-04.03.2021.pdf>

96 Premier Ministre, Circulaire n°6264/SG du 27 avril 2021 relative à la politique publique de la donnée, des algorithmes et des codes source : <https://www.legifrance.gouv.fr/download/pdf/circ?id=45162>

97 Voir la liste complète ici : <https://www.data.gouv.fr/fr/datasets/liste-des-administrateurs-ministeriels-des-donnees/>

- Une éducation à la citoyenneté numérique au sens large : s'éduquer sur ce que sont les données de santé, à quoi elles servent et peuvent servir. Familiariser les citoyens à l'usage des outils faisant appel aux données de santé développés par les services publics (DMP, ENS) et privés, et les accompagner dans ces usages si nécessaire. Les mettre en capacité de reconnaître les bons et les mauvais usages de leurs données de santé.
- Une éducation sanitaire : expliquer l'intérêt d'avoir des données de santé hiérarchisées et traitées à bon escient. Cette approche se retrouve notamment au travers de l'application TousAntiCovid, qui comprend un centre d'informations relatives à la situation épidémiologique et aux actualités en lien avec la lutte contre l'épidémie (ex. les mesures mises en place par les autorités nationales et locales).
- Une éducation thérapeutique : accompagner les patients ayant un intérêt particulier à utiliser des solutions comme des dispositifs médicaux connectés, dans leurs usages. Un exemple notoire est la prise en charge des patients atteints de pathologies chroniques qui sont équipés de dispositifs médicaux connectés. Ces derniers doivent très rapidement apprendre à lire leurs données de santé et à les interpréter. Une acculturation rendue possible notamment grâce à l'assistance thérapeutique délivrée par les professionnels de santé dans le cadre du parcours de soins.

Afin de garantir un égal accès à la santé, il est toutefois impératif que les efforts d'éducation prennent en compte les différents niveaux de littératie au sein de la population. Par exemple, consulter ses données de santé sur une plateforme en ligne comme Mon Espace Santé ou (pour le moment) le Dossier médical partagé (DMP) requiert déjà une certaine littératie numérique, au-delà de la problématique même des données : navigation sur internet, gestion de mots de passe. Certains citoyens ne possèdent pas ce niveau de maîtrise. À l'inverse, un patient diabétique, par exemple, qui est habitué à gérer sa pathologie au quotidien à l'aide d'un dispositif connecté à une application, aura sans doute plus de facilité à accéder à des services de santé en ligne et à les utiliser. Selon le sondage OpinionWay précité, « l'utilisation des outils numériques de santé est plus ancrée chez les populations habituées au monde digital, mais aussi chez certaines populations ayant une santé plus fragile (personnes en situation de handicap, bénéficiaires

de l'ALD⁹⁸, patients avec des visites fréquentes chez le médecin...) ou encore situées dans les déserts médicaux. »⁹⁹ Comme illustré par l'exemple de la prise de rendez-vous sur des plateformes en ligne pour la vaccination contre le Covid-19, ces inégalités d'acculturation au numérique peuvent entraîner une inégalité d'accès aux soins.

Il apparaît en outre indispensable de mettre en place un accompagnement spécifique des personnes les plus isolées, par exemple par le biais des maisons France Services¹⁰⁰, qui constituent des relais dans les territoires et complètent la stratégie nationale « Ma Santé 2022 ». À cet égard, lors de la présentation de son plan, la ministre de la Transformation et de la Fonction publiques a insisté sur la nécessité pour l'administration de profiter de sa numérisation pour proposer des démarches plus simples, plus ergonomiques et plus rapides, soulignant toutefois qu'« il ne s'agit pas de faire du 100 % numérique, mais de faire du numérique 100 % de qualité avec toujours une alternative »¹⁰¹. Il ne faut pas non plus minimiser certains obstacles techniques persistants, comme le manque d'interopérabilité entre systèmes d'information et logiciels métiers. Si, depuis 2011, seulement un peu plus de 9 millions de dossiers médicaux partagés (DMP) ont été ouverts (pour un objectif de 40 millions d'ici à 2022), c'est aussi du fait du manque d'interopérabilité des systèmes d'information en santé¹⁰².

Diffuser au sein de la société une culture des données de santé passe inévitablement par une sensibilisation à tous les temps de la vie. En premier lieu, elle doit être incarnée au plus haut niveau de l'État. Sans un portage politique fort, on risque de rester à des discours portés par des ultra-spécialistes. Il est dès lors primordial,

98 L'allocation d'affection longue durée (ALD) concerne toute personne souffrant de maladie chronique. Il s'agit d'une prise en charge à 100% par l'Assurance Maladie des soins qui concernent la maladie chronique.

99 Ministère des Solidarités et de la Santé, Les Ateliers Citoyens du numérique en santé, *Rapport Phase 2 : Les Français et le virage numérique en santé*, 2020, p. 27 : https://esante.gouv.fr/sites/default/files/media_entity/documents/ateliers-citoyens-rapport-phase02-vdef-2020-11-17-web.pdf
100 Voir : <https://www.cohesion-territoires.gouv.fr/france-services>

Dans son rapport d'information sur le dossier médical partagé (DMP) et les données de santé, le député Cyrille Isaac-Sibille suggérait d'ailleurs de mobiliser les maisons France Services pour garantir aux personnes éloignées du numérique d'avoir accès à leur DMP.

101 Ministère de la Transformation et de la Fonction Publiques, « 400 jours pour accélérer la transformation numérique de l'État », Dossier de presse, 4 mars 2021 : <https://www.transformation.gouv.fr/files/presse/Dossier-de-presse-400-jours-accelerer-transformation-numerique-etat-04.03.2021.pdf>

102 Cyrille Isaac-Sibille (juillet 2020), *Rapport d'information déposé en application de l'article 145 du Règlement, par la Commission des Affaires sociales, en conclusion des travaux de la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale sur le dossier médical partagé et les données de santé*, 124 pp. : <https://www.vie-publique.fr/rapport/275971-rapport-sur-le-dossier-medical-partage-et-les-donnees-de-sante>

sur des sujets aussi cruciaux que le numérique en santé, que les décideurs publics adoptent des messages clairs et compréhensibles. La question des données de santé et de leur exploitation ne se limite pas à des enjeux d'ordre technologique ou liés à de potentielles dérives. Or, ces derniers ont largement dominé les débats récents, que ce soit autour de l'application StopCovid (interrogations autour de la technologie Bluetooth, polémique concernant la possibilité d'utiliser l'application développée par Apple et Google, crainte d'une surveillance généralisée et d'un usage contraint) ou du *Health Data Hub* (hébergement des données par Microsoft Azure). En complément à ces aspects, qui d'un point de vue citoyen méritent tout autant d'être expliqués et compris, l'acculturation au numérique en santé doit être abordée sous le prisme de la santé. Cela passe, par exemple, par l'identification de cas d'usages simples et concrets, des *success stories* susceptibles de parler à tous (ex. la plateforme ViteMaDose, qui permet de trouver des créneaux de vaccination contre le Covid-19), afin de familiariser les citoyens aux données de santé et à leurs usages. Au vu de l'importance des enjeux, ces efforts doivent être massifs et passer par des campagnes grand public, comme cela a été fait dans le cadre de la lutte contre le Covid-19. L'enjeu est également de parvenir à toucher les publics les plus éloignés de ces sujets, notamment les jeunes en bonne santé, qui se sentent peu concernés. Pour cela, la communication mise en place doit être pensée en fonction des différents publics ciblés. Les réseaux sociaux sont, par exemple, un canal important de communication auprès des jeunes publics.

Que ce soit dans le monde professionnel ou à l'école, les visites médicales, qui sont aussi des objets de prévention, sont également des temps qui pourraient participer de cette sensibilisation générale au numérique en santé. À cet égard, l'éducation aux données mérite d'être renforcée à l'école, et ce dès le plus jeune âge. Dans cette logique, le *Health Data Hub* coopère avec l'Éducation nationale pour que la question des données soit intégrée à la notion de numérique dans les cours d'enseignement moral et civique, et travaille également à la mise à disposition des enseignants d'outils autour des données. Une approche qui mériterait d'être déployée à grande échelle en élargissant la base des acteurs impliqués (le *Health Data Hub* n'ayant pas vocation à porter la politique d'éducation aux données en France).

LA NÉCESSAIRE MONTÉE EN PUISSANCE DES ACTEURS DU SYSTÈME DE SANTÉ SUR CES SUJETS

Certains acteurs clés du système de santé doivent également monter en puissance sur ce défi d'acculturation, et être revalorisés à ce titre. De ce point de vue, tout n'est pas à réinventer. Les associations et communautés de patients pourraient, par exemple, constituer un vecteur d'acculturation à fort potentiel. Or, les auditions

menées dans le cadre de ce travail ont révélé que ces dernières étaient dans l'ensemble très peu structurées en ce domaine. Il faut donc encourager les associations de patients à se saisir des enjeux liés aux données de santé, les former, et les inciter à se mettre en relation dans une logique d'apprentissage mutuel. Les plus matures sur le sujet du numérique en santé pourraient ainsi participer de la diffusion de bonnes pratiques en termes d'appropriation des données, qui pourraient ensuite être répercutées par chaque association auprès de ses membres. Cette mise en capacité des associations de patients doit également permettre de donner un nouvel élan à la démocratie sanitaire, en renforçant leur rôle dans les décisions afférentes à la politique du numérique en santé.

En outre, un certain nombre de métiers, à l'instar des médecins, des infirmiers, des pharmaciens, ou encore des acteurs du secteur médico-social et paramédical (ex. les aides-soignants), sont *de facto* déjà des médiateurs en santé. Demain, ils ont vocation à accompagner les citoyens dans leurs usages du numérique en santé. À cet égard, les pharmaciens et les infirmiers pourraient, par exemple, avoir un rôle ciblé sur certaines pathologies, certains dispositifs connectés ou certains types de télésurveillance. Il ne s'agit pas là de créer de nouveaux métiers, mais d'une évolution des métiers existants. Pour le déploiement de l'ENS, par exemple, la Délégation ministérielle du numérique en santé (DNS) préconise de « *s'appuyer sur les généralistes, les spécialistes et les pharmaciens d'officine qui bénéficient d'un niveau de confiance élevé et sont par ailleurs déjà familiers du système des outils partagés* »¹⁰³.

« Le professionnel de santé est notre premier interlocuteur : c'est à lui de nous garantir la transparence et le cadre qui entourent l'usage de ces données (possibilité d'opt-out, etc.). Il y a un environnement anxiogène sur l'usage des données (StopCovid, actualité générale). Il faut remettre le professionnel de santé au cœur de tout cela, en lui donnant les moyens et la formation nécessaires. »

Nesrine Benyahia,

CO-PRÉSIDENTE DU COLLÈGE NUMÉRIQUE, SOCIÉTÉ FRANÇAISE DE SANTÉ DIGITALE

103 Ministère des Solidarités et de la Santé, Les Ateliers Citoyens du numérique en santé, *Rapport Phase 2 : Les Français et le virage numérique en santé*, 2020, p. 27 : https://esante.gouv.fr/sites/default/files/media_entity/documents/ateliers-citoyens-rapport-phase02-vdef-2020-11-17-web.pdf

Le numérique en santé, *de facto*, aura un impact sur les professions du secteur, qui verront leur champ de compétences s'élargir ou se restreindre. Il faut que chaque profession se saisisse de cet enjeu pour se réinventer, et que soit organisée une forme d'accompagnement à la conduite du changement à leur égard. C'est précisément dans cette optique que s'inscrit par exemple la création récente du statut d'assistant médical pour les médecins libéraux¹⁰⁴.

Certains métiers, à l'instar des médecins, des infirmiers, des pharmaciens et autres acteurs du secteur médico-social et paramédical, doivent non seulement être davantage accompagnés dans l'accomplissement de leurs missions, mais également faire l'objet d'une revalorisation le cas échéant, si ces dernières s'étendent et/ou évoluent en matière de responsabilité. Face à la rapide évolution des solutions numériques appliquées à la santé, à la multiplicité des offres disponibles en termes de logiciels métiers, aux évolutions récentes du cadre juridique, ou encore aux exigences à remplir en matière de référentiels d'interopérabilité et de sécurité, certains professionnels de santé peuvent se sentir démunis. Cela vaut autant pour le milieu hospitalier que pour la médecine de ville. Bien que cette injonction soit systématiquement évoquée depuis plusieurs années, il convient de rappeler ici la nécessité d'intégrer dans les cursus de formation en santé, que ce soit au niveau de la formation initiale ou de la formation continue (qui est, du reste, quasi inexistante dans ce domaine), des notions afférentes à l'utilisation du numérique et des données dans le domaine de la santé. Le 22 février dernier, le ministre des Solidarités et de la Santé, Olivier Véran, et le secrétaire d'État chargé de la Transition numérique et des Communications électroniques, Cédric O, ont annoncé que « *la sensibilisation à la cyber sécurité sera intégrée dans tous les cursus de formation des acteurs en santé, afin de conforter les pratiques 'd'hygiène numérique'* »¹⁰⁵. S'il s'agit là d'un pas dans la bonne direction, la cybersécurité est loin d'être l'unique aspect auquel les acteurs de la santé méritent d'être sensibilisés. Pour combler ces lacunes dans la formation, l'Association nationale des étudiants en pharmacie de France (ANEPF) a élaboré une maquette d'enseignement à la e-santé qui pourrait être intégrée à la formation initiale de tous les étudiants en santé. Parmi les propositions énumérées dans le document : intégrer dans la formation initiale des étudiants en santé

un module commun d'initiation au numérique en santé, créer un ensemble de formations continues pour l'exercice de santé numérique spécifique à chaque profession de santé, diversifier l'offre de stages hospitaliers et en industrie afin de sensibiliser les étudiants aux nouveaux métiers du numérique, ou encore inciter à la création d'un master ou d'un diplôme universitaire d'e-santé¹⁰⁶. Les professionnels de santé doivent également être accompagnés dans la pratique sur certains usages comme les logiciels métiers (référentiels de sécurité et d'interopérabilité à adopter).

Outre cette montée en puissance des acteurs du système de santé et une évolution de certains métiers, il y a un accompagnement plus général à penser afin de sensibiliser la population dans son ensemble (y compris les moins connectés) aux enjeux du numérique en santé, et *a fortiori* aux données de santé. On peut souligner à cet égard l'initiative de l'Agence nationale pour la cohésion des territoires (ANCT) visant à former 3 000 « conseillers numériques » d'ici à juin 2022¹⁰⁷. Une fois formés, ces conseillers ont vocation à être déployés prioritairement au sein des antennes France Services sur l'ensemble du territoire national. À l'heure où des pans entiers des politiques publiques sont digitalisés, en particulier dans la santé, cette politique de médiation numérique mériterait d'être massifiée afin de répondre à ces nouveaux enjeux.

UNE DIFFUSION QUI PASSE AUSSI PAR LA PRATIQUE

Cette acculturation passera également par les usages. À titre d'exemple, on peut citer l'application StopCovid qui, parce qu'elle avait été initialement conçue et promue essentiellement comme un outil de traçage des cas contact, a été un échec du point de vue de l'adoption dans un premier temps. Ce n'est que sous sa deuxième version, TousAntiCovid (l'application comporte désormais des rubriques d'information sur l'épidémie, des conseils personnalisés, la carte des laboratoires de dépistage et des centres de vaccinations

104 « Création des assistants médicaux : les textes sont parus ! », *Infirmiers.com*, 21 août 2019 : <https://www.infirmiers.com/actualites/revue-de-presse/creation-assistants-medicaux-textes-parus.html>

105 Ministère des Solidarités et de la Santé, « Sécurité des réseaux informatiques des établissements de santé : le Gouvernement renforce sa stratégie », Communiqué de presse, 22 février 2021 : <https://solidarites-sante.gouv.fr/actualites/presse/communiques-de-presse/article/securite-des-reseaux-informatiques-des-etablissements-de-sante>

106 Association Nationale des Étudiants en Pharmacie de France (2021), *Enseignement Supérieur et Numérique. Contribution Innovations Pédagogiques et Évolution des Études de Pharmacie*, 26 pp. : https://drive.google.com/file/d/117Hnu-IL_cKIdAXEJITxJiqgCRmN3h27/view

107 « L'Afpa et Simplon.co vont former près de 3000 conseillers numériques d'ici juin 2022, sur tout le territoire », *Labo Société Numérique*, 20 avril 2021 : <https://labo.societenumerique.gouv.fr/2021/04/20/lafpa-et-simplon-co-vont-former-pres-de-3000-conseillers-numeriques-dici-juin-2022-sur-tout-le-territoire/>

les plus proches, un accès aux attestations de déplacement, des informations concernant l'éligibilité des individus aux vaccins, les certificats de tests et de vaccinations, etc.), qu'une partie plus importante de la population l'a adoptée. L'apport en matière d'usage n'y est sans doute pas pour rien. Dans cette même logique, le « portail patient » estonien¹⁰⁸, équivalent au futur ENS, permet aux citoyens de consulter l'historique de leurs consultations, leurs résultats d'analyses médicales (y compris des tests Covid), leurs comptes-rendus de consultations et d'hospitalisations, leur carnet de vaccinations, la liste des traitements prescrits par les professionnels de santé qu'ils ont consultés, mais également de prendre un rendez-vous médical, d'obtenir des certificats médicaux nécessaires au renouvellement de leur permis de conduire, et d'indiquer leurs préférences relatives à leur santé (ex. En cas d'accident, acceptez-vous de recevoir une transfusion sanguine ? En cas de décès, désirez-vous donner vos organes ? etc.). En France, l'ENS, qui sera accessible pour tous les citoyens à partir du 1er janvier 2022, est actuellement en construction. S'est posée la question de la stratégie à adopter. Est-il plus judicieux de viser une approche progressive, en proposant dans un premier temps un nombre de services limités, ou au contraire miser sur des avancées massives englobant de nombreux services qui concernent l'ensemble de la population, afin de combler le retard ? Le choix de la Délégation ministérielle au numérique en santé (DNS) semble se porter sur la seconde option. L'ENS sera ouvert pour tous, dès la naissance, selon la logique de l'*opt-out*¹⁰⁹, et constituera un socle général adressé à tous. Une autre option aurait pu être de proposer des services par pathologie, pour garantir un certain niveau d'adoption par de grandes communautés de patients, avant d'envisager un élargissement des services disponibles à l'ensemble de la population. Si le choix de la DNS s'est porté sur le développement d'un socle général, comportant de nombreux services adressés à l'ensemble des citoyens dès son lancement, il faudra toutefois veiller à ce que cette approche « massive » de l'ENS tienne compte des différents « types » de citoyens. Si l'approche est globale, l'accompagnement, lui, doit être progressif et adapté à chacun.

¹⁰⁸ Voir : <https://www.digilugu.ee/login?locale=en>

¹⁰⁹ « *Opt-out* » est un terme appartenant à l'origine au domaine législatif et de la publicité. Il est utilisé pour décrire une situation dans laquelle un individu est le destinataire d'un service « par défaut », c'est-à-dire sans y avoir consenti mais sans s'y être opposé. Pour en savoir plus, voir : <https://www.cnil.fr/fr/cnil-direct/question/opt-opt-out-ca-veut-dire-quoi>

« MON ESPACE SANTÉ » : UN OUTIL À LA DISPOSITION DES CITOYENS POUR ACCÉDER ET DONNER ACCÈS À LEURS DONNÉES DE SANTÉ

La loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé prévoit la création automatique d'un Espace numérique de santé (ENS) pour tous les usagers du système de soins, sauf opposition de l'usager ou de son représentant légal, et ce, au plus tard en janvier 2022.

Baptisé « Mon Espace Santé », cet ENS contribuera à l'animation de l'écosystème numérique en santé en France par la publication d'un catalogue de services numériques en santé développés par les acteurs publics et privés et référencés par la puissance publique (portail patient des hôpitaux, services numériques à destination des usagers développés par les éditeurs de logiciels et d'applications et les start-ups, applications et dispositifs médicaux connectés développés par les industriels, etc.).

À travers son ENS, l'usager pourra accéder à :

- son dossier médical partagé (DMP), espace de stockage sécurisé des données de santé (synthèse médicale, mesures de santé, carnet de vaccinations, comptes-rendus médicaux, comptes-rendus d'examen de biologie médicale, ordonnances, soins remboursés, copies de radiologie, etc.) ;
- une messagerie sécurisée permettant des échanges d'informations et de documents (ordonnances, photos, etc.) avec les professionnels qui interviennent dans son parcours de soins ;
- un « agenda-santé » permettant de consolider les différents événements de santé : rendez-vous médicaux, hospitalisations, rappels, etc. Ces événements pourront être alimentés par les services de prise de rendez-vous, les portails des établissements et l'usager lui-même ;
- un catalogue de services référencés par la puissance publique (le « store » ENS) : l'usager pourra choisir de donner accès aux données, y compris de santé, de son ENS aux applications de son choix et inversement d'enregistrer les données issues de ces applications dans son ENS.

Source : sesam-vitale.fr/espace-numerique-de-sante

SENSIBILISER LE SECTEUR NUMÉRIQUE AUX ENJEUX PROPRES AUX DONNÉES DE SANTÉ

Imaginer des solutions de « santé numérique » (ou de e-santé) ne revient pas simplement à prendre des outils ou raisonnements numériques et à les appliquer au secteur de la santé. Cela nécessite de développer des connaissances sur l'écosystème de la santé et les enjeux auxquels il fait face, et auxquels le numérique pourrait éventuellement répondre.

« Il faut que l'on change le point de vue et que l'on passe d'un angle "numérique" à un angle "santé". Le meilleur moyen d'accéder au marché est, avant l'innovation numérique, la réponse aux besoins des médecins et des patients. »

Yann-Maël Le Douarin,

CONSEILLER MÉDICAL TÉLÉSANTÉ, DGOS, MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

En e-santé, le point de départ ne doit pas être la technologie, mais bien la santé. C'est parce qu'un enjeu spécifique dans la chaîne de santé est identifié, qu'il peut être intéressant d'y apporter une réponse basée sur des solutions numériques, et pas l'inverse. Une telle démarche demande un effort d'acculturation du secteur numérique aux enjeux liés à la santé.

Comme dans de nombreux autres secteurs, les métiers issus du monde numérique « pur », à l'instar des *data scientists*, investissent petit à petit la sphère de la santé. Or, manier des données liées à la santé des individus nécessite des connaissances métiers extrêmement fines. Il s'agit non seulement de savoir interpréter les données, mais également de compren-

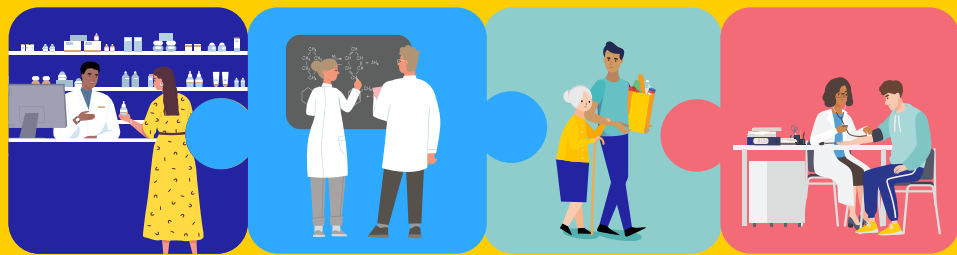
dre les *process* métier qui les entourent : qui les génère ? Qui les exploite ? À quelles fins ? Par exemple, dans le cadre de la lutte contre l'épidémie de Covid-19, définir la bonne métrique pour attester que la vaccination se déroule bien ou non, nécessite des compétences qui vont au-delà de la seule *data science*. La métrique doit-elle être le nombre d'injections réalisées ? Le nombre de deuxièmes injections ? Trancher ce genre de questions ne relève pas uniquement de compétences en termes de statistique, de logistique ou de données, mais également en santé (ex. épidémiologie, infectiologie-virologie, etc.).

Par ailleurs, il ne faut pas oublier que les données de santé n'ont pas été initialement conçues à des fins d'analyse ou de recherche. Celles contenues dans le SNDS, par exemple, peuvent être particulièrement difficiles à appréhender au premier abord. Les analyser nécessite un travail d'apprentissage qui peut prendre plusieurs mois. Cette dimension est d'autant plus importante à souligner que la capacité à appréhender ces données joue souvent un rôle majeur dans l'obtention des autorisations de traitement. Ainsi, les expressions de besoins d'accès aux données du SNDS formulées par des individus familiers avec la forme de ces dernières et avec ce qu'elles peuvent permettre, peuvent être validées sous deux mois. À cet égard, les professionnels des données de santé, qui, eux, savent appréhender ces données, pourraient jouer un rôle dans l'acculturation des acteurs du numérique à la santé. Cela nécessite de construire des ponts entre ces deux mondes, qui travaillent sur les mêmes sujets sans forcément se rencontrer.

In fine, ces efforts d'acculturation aux données de santé tout au long de la chaîne sanitaire doivent permettre une clarification des rôles entre les différents acteurs impliqués dans le numérique en santé. Mais si se saisir des données de santé constitue un fort enjeu d'acculturation, il s'agit également d'un enjeu de gouvernance. Pour l'heure, certains aspects techniques et juridiques sur lesquels il convient de réaliser des arbitrages rendent complexe cette dernière.

PARTIE 3

REDÉFINIR LA GOUVERNANCE DES DONNÉES POUR UN SYSTÈME DE SANTÉ PLUS EFFICIENT ET PLUS DÉMOCRATIQUE



En parallèle à l'indispensable montée en puissance de l'ensemble des acteurs de la chaîne sanitaire sur le sujet des données de santé, se saisir de ces données nécessite de donner plus de clarté à leur gouvernance. Redéfinir la gouvernance des données de santé, c'est d'une part clarifier le rôle des différents acteurs impliqués dans leur production, collecte, partage et utilisation, et d'autre part clarifier les modalités (techniques, juridiques) de production, de collecte, de partage et d'utilisation de ces données.

CLARIFIER LE PILOTAGE DE LA POLITIQUE PUBLIQUE DES DONNÉES DE SANTÉ

RENFORCER LA COLLABORATION DES ACTEURS IMPLIQUÉS DANS LA GOUVERNANCE DES DONNÉES DE SANTÉ

Redéfinir la gouvernance des données de santé passe dans un premier temps par une clarification de la politique publique en la matière. Pour être efficace, la gouvernance des données de santé doit associer l'ensemble des acteurs de la chaîne de santé, jusqu'aux citoyens, et prendre en compte l'intérêt que peuvent représenter ces données pour les différents maillons de la chaîne. CHU, ARS, ministères (voire même différentes entités au sein d'un même ministère), professionnels de santé, mutuelles, citoyens, patients et associations de patients, industriels, tous n'ont pas le même rapport aux données et n'en ont pas les mêmes usages. Il convient donc de prendre en considération ces différents intérêts ainsi que certaines particularités territoriales.

À court terme, il convient de faire en sorte que le dialogue circule entre les différents acteurs, et il y a là, en partie, une question de management. Tous les blocages ne relèvent pas, en effet, de décisions politiques. Des blocages surviennent également car les dialogues ont lieu à des niveaux hiérarchiques qui ne sont pas optimaux. Afin de faire circuler la parole entre les différents acteurs du système, une *task force* transversale dédiée aux questions liées au traitement des données de santé pourrait être mise en place, dont le rôle serait d'assister les acteurs comme les ARS et la HAS, et de leur apporter des connaissances spécifiques pour accompagner leur montée en puissance.

Cette task force constituerait une sorte de PEReN¹¹⁰ des données de santé, mais dont les prérogatives ne se limiteraient pas aux enjeux de régulation. Elle pourrait s'inspirer de la logique d'infusion qui émerge dans le domaine de la régulation du numérique, en encourageant l'émulation sur différentes expertises propres à divers acteurs, comme par exemple l'ANSSI, la CNIL et des statisticiens de la santé.

Pour que cette gouvernance multipartite fonctionne, il est nécessaire que les différents acteurs du système communiquent davantage et que le rôle de chacun soit précisément défini. Or, au regard des auditions menées dans le cadre de cette étude, ce n'est pas toujours le cas. Si encourager ces acteurs à coopérer davantage peut constituer une solution de court terme, sur le long terme, il conviendra de mieux définir leurs missions, ce qui ne peut se faire par décret et exige des arbitrages collectifs.

INCITER LES ACTEURS DE LA CHAÎNE DE SANTÉ AU PLUS GRAND PARTAGE DE LEURS DONNÉES

Piloter la politique publique des données de santé oblige également à penser et instaurer des mécanismes d'incitation au partage de ces données. Cela passe notamment par la mise en place d'intermédiaires de confiance entre les acteurs susceptibles de mettre leurs données de santé à disposition et ceux désireux de les réutiliser. Parmi les formes que peuvent prendre ces intermédiaires, il y a les *data trusts*¹¹¹ (dont les contours précis restent encore à définir). À travers un *data trust*, les données générées par un individu ou une entité sont confiées à un tiers de confiance, le *data trustee*, qui les gère entièrement à sa place en respectant ses volontés (avec qui partager, dans quel but, etc.). C'est en quelque sorte dans cette optique que s'inscrit le *Health Data Hub*, au travers duquel l'État joue le rôle de tiers de confiance pour les acteurs qui acceptent de mettre leurs données à disposition via la plateforme (et donc, indirectement, pour les citoyens). Mais malgré les efforts consentis dans le

cadre de la stratégie « Ma Santé 2022 », de nombreux établissements de santé restent réticents face à l'idée de mettre leurs données à disposition au sein de la plateforme nationale. Dans le même temps, des plateformes de données de santé voient le jour au niveau régional voire inter-régional (voir Tableau 2). Ces deux logiques ne vont pas nécessairement à l'encontre l'une de l'autre et peuvent même se compléter. Le développement de hubs régionaux et inter-régionaux permet une valorisation des données de santé à une échelle certes plus réduite que le *Health Data Hub*. Mais il peut aussi assurer des délais d'obtention des autorisations de traitement des données à des fins de recherche moindres que si toutes les requêtes étaient centralisées au niveau national. *In fine*, l'important est que les initiatives prises de part et d'autre puissent se rejoindre. Un minimum de coopération entre les différents hubs de données de santé qui se développent est donc nécessaire. Cela peut par ailleurs être un bon moyen d'éviter les redondances en matière d'initiatives.

« On a déjà un certain nombre de grosses structures qui se regroupent dans le Grand-Est ou le Grand-Ouest, pour monter des entrepôts de données régionaux ou interrégionaux. Il doit y avoir une complémentarité entre ces derniers et le Health Data Hub (HDH). Le HDH doit s'appuyer sur les compétences et les entrepôts déjà mis en place. »

Cécile Chevance,

DIRECTRICE DU PÔLE FINANCE/FHF DATA À LA FÉDÉRATION HOSPITALIÈRE DE FRANCE

Afin d'encourager une plus grande circulation des données publiques et privées au niveau de l'Union européenne, le règlement européen sur la gouvernance des données (*Data Governance Act*) proposé par la Commission européenne en novembre 2020¹¹² entend professionnaliser « l'altruisme en matière de données », qui n'est selon l'exécutif européen pas suffisamment

110 Le PEReN est le « pôle d'expertise de la régulation numérique », un service à compétence nationale rattaché aux ministères de la Culture et de l'Économie et au secrétariat d'État au Numérique. Il a vocation à mutualiser les expertises dans un centre de service partagé, la régulation des plateformes numériques étant un sujet transverse à de nombreuses administrations et autorités administratives indépendantes.

111 Open Data Institute, « What is a data trust? », 10 juillet 2028 : <https://theodi.org/article/what-is-a-data-trust/>

112 Commission européenne, « Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données) », COM/2020/767 final, 25 novembre 2020 : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020PC0767&from=FR>

mobilisé, et encourager son utilisation à grande échelle. Le texte prévoit la possibilité, pour les tiers de confiance qui se posent en intermédiaires, de s'enregistrer en tant qu'« organisation altruiste en matière de données reconnue dans l'UE » afin de renforcer la confiance dans leurs activités. Un modèle d'autant plus intéressant lorsqu'il s'agit d'échanger des données extrêmement sensibles comme les données de santé. Pour aller plus loin, cette démarche volontariste pourrait être complétée par une certification des tiers en question par la Commission européenne. Si cette possibilité n'a pas été retenue dans le texte, l'exécutif ne l'exclut toutefois pas.

Outre les *data trust*, l'instauration d'une relation de confiance peut également se matérialiser par le biais de **solutions contractuelles**. Certaines garanties, portant notamment sur la nature des données partagées, l'intention derrière leur réutilisation, d'éventuelles limites à cette réutilisation, ou encore des obligations afférentes à la transparence du traitement ou aux responsabilités incombant à son responsable, peuvent être incluses dans des clauses spécifiques des contrats de partage de données. Une telle pratique permet une protection accrue des deux parties, plus de clarté et de sécurité dans les échanges, entraînant, *in fine*, une plus grande incitation au partage de données. On peut par exemple imaginer ce genre de clauses dans un contrat entre un professionnel de santé et son fournisseur de solutions numériques. Mais les acteurs impliqués ne possèdent pas nécessairement l'expertise nécessaire à la rédaction de telles clauses. Ces dernières ne sont par ailleurs pas toujours très claires. Afin de pallier ces difficultés, le *Support Centre for Data Sharing* de la Commission européenne propose, par exemple, une assistance juridique aux acteurs désireux de mettre en place un partage de données. L'organisation a notamment développé un « assistant de contractualisation » qui, en fonction des informations renseignées par les deux parties (l'acquéreur et le fournisseur des données), génère automatiquement un contrat de licence personnalisé pour le partage des données en question. Un dispositif similaire pourrait très bien être imaginé au niveau national, dans une démarche interministérielle rassemblant les différents ministères pertinents, à savoir le ministère des Solidarités et de la Santé (et en particulier la Délégation au numérique en santé), le ministère de l'Enseignement Supérieur et de la Recherche, et le ministère de l'Économie, des Finances et de la Relance. La plateforme G_NIUS, mise en place par le ministère des Solidarités et de la Santé, en partenariat avec l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), l'Assurance Maladie, Bpi-

france, la CNIL et la HAS¹¹³, pourrait accueillir des contrats types ainsi qu'un assistant de contractualisation tel qu'imaginé par le *Support Centre for Data Sharing* européen.

Penser des mécanismes d'incitation au partage de données de santé, c'est également s'attaquer aux logiques de thésaurisation des données adoptées par certains acteurs de la chaîne de santé. À ce sujet, il convient de rappeler la distinction entre deux notions clés : « partager » des données et « donner accès » à des données. Si, dans le premier cas, l'utilisateur possède une copie physique des données sur son serveur, il ne peut dans le second cas que les exploiter par un accès sécurisé au serveur du producteur, sans en garder une copie physique. À cet égard, le rapport issu de la « mission pour une politique publique de la donnée » (dite « mission Bothorel ») déplore le fait que de nombreux acteurs « *ne considèrent pas même l'éventualité de partager de manière limitée et sécurisée certaines de leurs données* »¹¹⁴. Ce constat souligne encore une fois l'importance de faire de la pédagogie auprès de tous les acteurs impliqués dans la production et le traitement de données de santé. Le problème n'est pas spécifique à la santé et concerne tous les écosystèmes reposant sur le partage de données entre acteurs. Toutefois, la santé reste un secteur où la notion de valorisation des données est mal perçue. Il existe par ailleurs des solutions techniques permettant une exploitation de données d'origines multiples, sans que l'utilisateur y ait directement accès. C'est le cas, par exemple, du *machine learning* multipartite. Cette technologie permet à plusieurs entités qui souhaitent collaborer pour entraîner un modèle d'intelligence artificielle d'aboutir à un modèle en mettant leurs données en commun, mais sans pour autant que chaque acteur ait accès aux données de ses partenaires. L'utilisation de techniques dites « d'informatique confidentielle » (ou de calcul confidentiel), peut également s'avérer intéressante. L'informatique confidentielle repose sur les capacités des dernières générations de processeurs, et permet, grâce à un processus de chiffrement, de partager des données sans y donner accès. De telles solutions mériteraient d'être encouragées par la puissance publique afin de lever les réticences de certains acteurs au partage de leurs données.

¹¹³ La plateforme G_NIUS vise à stimuler les innovations du numérique en santé. Elle propose des outils destinés à aider les entrepreneurs à décrypter la réglementation en matière de e-santé, à identifier les acteurs de l'écosystème et leurs rôles, et à en savoir plus sur les sources de financement accessibles.

¹¹⁴ Gouvernement (Mission Bothorel), *Pour une politique publique de la donnée*, Décembre 2020, p. 9 : https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publicque_de_la_donnee_-_23.12.2020_-_0.pdf

INSCRIRE LA POLITIQUE PUBLIQUE DES DONNÉES DE SANTÉ DANS LA STRATÉGIE EUROPÉENNE

La politique publique des données de santé française doit également s'inscrire dans la stratégie européenne, qui va être amenée à largement se développer dans les années à venir.

En avril 2018, la Commission européenne a adopté une communication portant sur la transformation numérique des services de santé et de soins dans le marché unique numérique¹¹⁵. Celle-ci vise trois objectifs : l'accès sécurisé des citoyens aux données de santé et le partage de ces données avec d'autres États membres, l'amélioration de la qualité des données dans le but de faire progresser la recherche, la prévention des maladies et la personnalisation des soins de santé, et la promotion d'outils numériques pour l'autonomisation des citoyens et pour des soins centrés sur la personne. Dans la lignée de cette communication, l'exécutif européen a adopté une recommandation relative au format européen d'échange des dossiers de santé informatisés¹¹⁶. Son but : favoriser l'échange de ces dossiers d'un État membre à l'autre, en encourageant la mise en place d'un format d'échange commun. S'il est prévu que 22 États membres soient capables d'échanger ce genre de documents d'ici à la fin de l'année 2021 par le biais de la plateforme dédiée *eHealth Digital Service Infrastructure* (eHDSI), seules la Finlande et l'Estonie y sont, pour l'heure, parvenues. Il est donc primordial que le développement des plateformes nationales, à l'instar du futur ENS français, qui permettra à l'ensemble des citoyens d'accéder à leurs dossiers médicaux, prennent en compte les exigences européennes en matière d'interopérabilité des formats. Dans le cadre du projet européen *National Contact Point eHealth* (NCPeH), il est en outre prévu que d'ici à la fin de l'année 2021, tout professionnel de santé de l'espace européen puisse accéder au dossier médical d'un patient citoyen d'un autre pays. Pour la France, c'est l'Agence du numérique en santé (ANS) qui a été désignée point de contact national (*national contact point*) pour la e-santé. À ce titre, elle est connectée aux services de coordination de la Commission européenne et servira d'intermédiaire entre les demandes des NCPeH des autres pays et les infrastructures nationales telles que l'ENS.

Au-delà des documents (e-prescriptions, compte-rendu), l'exigence d'interopérabilité vaut également pour le format des données de santé de façon générale, qui devront, pour certaines, pouvoir être intégrées au futur espace européen commun des données de santé. À ce titre, il convient de noter qu'au travers du *Health Data Hub*, la France participe à l'action conjointe « espace européen des données de santé » (ou TEHDaS) lancée le 1er février 2021 et qui rassemble la Commission européenne et 26 États membres. L'objet de cette initiative est, à travers le partage des connaissances des différents acteurs impliqués, de produire des recommandations afférentes à la mise en œuvre de la future plateforme de partage des données de santé à l'échelle européenne. Enfin, la gouvernance des données de santé au niveau national s'inscrira dans le cadre le *Data Governance Act*, dont l'objectif est d'améliorer les conditions de partage des données dans le marché intérieur, en créant un espace harmonisé pour les échanges de données.

Si la politique publique des données de santé française est déjà bien inscrite dans la stratégie européenne, les acteurs qui restent réticents à l'utilisation de standards d'interopérabilité internationaux, doivent encore entendre cette nécessité.

DES ARBITRAGES TECHNIQUES ET JURIDIQUES INDISPENSABLES

RENFORCER L'ADOPTION DES RÉFÉRENTIELS TECHNIQUES D'INTEROPÉRABILITÉ ET DE SÉCURITÉ

Comme évoqué en première partie, leur hétérogénéité est une des caractéristiques principales des données de santé. Elles constituent un patrimoine éparpillé au sein d'une multitude de bases de données différentes, qui opèrent souvent en silos les unes par rapport aux autres et sont gérées par une grande diversité d'acteurs. Chaque acteur a ainsi adopté, au fil du temps, ses propres systèmes d'information et ses propres logiciels et procédés de recueil et de traitement des données. Ces dernières ne sont donc pas toujours standardisées, ce qui limite fortement leur exploitation.

115 Commission européenne, COM(2018) 233 final, 25 avril 2018, 17 pp. : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0233&from=EN>

116 Commission européenne, Recommandation 2019/243, 6 février 2019, 10 pp. : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019H0243&from=EN>

« Les données numériques de santé se trouvent aujourd'hui majoritairement sous un format « non structuré » pénalisant une exploitation à forte valeur ajoutée métier. L'évolution des systèmes d'information en santé vers la production et l'échange de données, notamment dans le cadre de l'alimentation du « Health Data Hub », impose de mettre en place une gouvernance et des outils pratiques pour la structuration des données numériques de santé et leur codage sémantique. »

Feuille de route stratégique du numérique en santé

Du point de vue des arbitrages techniques devant être opérés, le défi est donc, dans un premier temps, de faciliter le rapprochement de ces données issues de bases différentes, et ce sans faire fi des précautions en matière de sécurité et confidentialité que ces données sensibles exigent (voir la section intitulée « Un cadre légal strict, qui agit en gardien » du présent rapport). Cela passe, pour les acteurs participant au recueil de données de santé (professionnels et établissements de santé, éditeurs de logiciels, industriels de la santé, Assurance Maladie, etc.), par le respect de référentiels socles en matière de sécurité, d'interopérabilité et d'éthique (voir le Schéma 3 ci-après). En France, la responsabilité de développer ces référentiels revient principalement à l'Agence du numérique en santé (ANS).

L'utilisation et la généralisation de l'Identité Nationale de Santé (INS) fait ainsi partie des mesures phares de la stratégie « Ma Santé 2022 » du gouvernement. L'INS est un matricule identifiant (à chaque individu correspond une INS), qui permet que tout patient soit reconnu dans tous les systèmes informatiques de manière unique, assurant ainsi la continuité des parcours de soins. Son utilisation est obligatoire depuis le 1^{er} janvier 2021 et l'INS constitue désormais la clé de lecture pour opérer des rapprochements de personnes : toute donnée de santé doit être référencée avec l'identité INS. Malgré cette obligation, il semblerait que l'adoption de ce référentiel soit à la peine. Les échanges organisés dans le cadre de ce rapport ont, en effet, révélé que, six mois après l'entrée en vigueur de

l'obligation, son utilisation n'est pas systématique. Il n'est, par exemple, pas utilisé pour toutes les activités internes au sein de l'Assurance Maladie. Du fait de la difficulté technique que représente le fait de passer d'un référentiel à un autre, il existe, de façon générale, une réticence, de la part de certains établissements et professionnels de santé, à adopter ce nouveau référentiel. Alors que sa création a mobilisé de nombreux acteurs du système de santé pendant plusieurs années, le défi est désormais d'avancer vers une adoption massive de l'INS. L'Agence du numérique en santé y travaille, et a récemment lancé une campagne de communication à ce sujet, notamment via les réseaux sociaux¹¹⁷. Des plans d'actions régionaux sont également coordonnés par les Autorités régionales de santé (ARS), les Groupement régionaux d'appui au développement de l'e-Santé (GRADeS) et les Directeurs coordonnateurs de la gestion du risque (DCGDR), avec pour objectif que l'INS soit portée dans au moins 80 % des communications entre acteurs de santé d'ici fin 2022.

En complément à l'INS, qui constitue un référentiel de sécurité, l'Agence du numérique en santé (ANS) a également développé un cadre d'interopérabilité des systèmes d'information de santé (CI-SIS)¹¹⁸, qui vise à faciliter « la dématérialisation et l'homogénéisation des informations échangées, partagées, tout en respectant l'autonomie des systèmes d'information de santé »¹¹⁹. Le CI-SIS constitue ainsi un document de référence, qui propose des règles techniques et sémantiques, destinées aux éditeurs et porteurs de projets numériques en santé, afin de favoriser le partage et l'échange de données de santé. En d'autres termes, il s'agit de s'assurer que les différents acteurs parlent le même langage, ce qui, *in fine*, devrait grandement faciliter les appariements de données. À cet égard, l'Agence du numérique en santé demande aux industriels de renseigner l'outil Convergence¹²⁰ pour apprécier leur conformité à ce cadre.

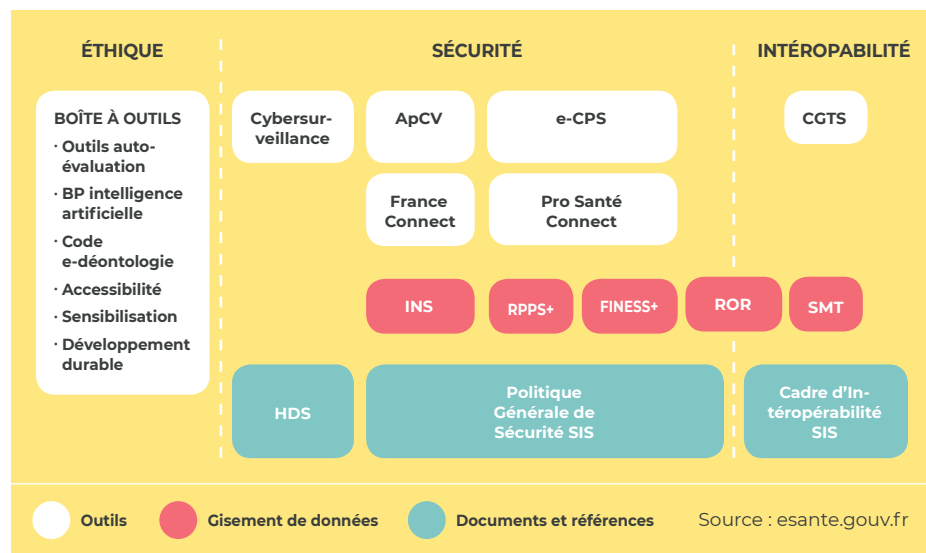
117 Par exemple, via LinkedIn : https://www.linkedin.com/posts/agence-du-numerique-en-sante_identifiant-national-de-sant%C3%A9-devient-l-activity-6785933231482126336-kuoo/

118 Voir : <https://esante.gouv.fr/interopabilite/ci-sis>

119 ANS, « Interopérabilité, pierre angulaire de la croissance en e-santé » : <https://esante.gouv.fr/interopabilite>

120 Voir : <https://convergence.esante.gouv.fr/>

SCHÉMA 3 - LES RÉFÉRENTIELS SOCLES APPLICABLES AUX DONNÉES DE SANTÉ EN FRANCE



Si l'entrée en vigueur de ces référentiels constitue déjà un accomplissement, il convient en effet de maintenir un niveau d'incitation soutenu afin que ceux-ci soient massivement adoptés. Des leviers ont précisément été pensés à cette fin. Au niveau des infrastructures numériques des établissements de santé, l'incitation peut notamment passer par une obligation pour ces derniers de respecter les référentiels d'interopérabilité dans leurs appels d'offres. L'obligation d'interopérabilité s'impose également aux industriels producteurs de logiciels et de dispositifs médicaux connectés. La HAS et le Comité économique des produits de santé (CEPS), qui négocie les prix desdits outils, sont très attentifs au respect de ces dispositions et tendent à en faire un critère d'évaluation. Enfin, il convient de ne pas oublier les professionnels de la médecine de ville, eux aussi concernés par cette mise en conformité, notamment pour ce qui est de leurs logiciels métier. Afin de les assister dans la modernisation et l'informatisation de leurs cabinets, l'Assurance Maladie a mis en place le « forfait structure », une aide financière à deux volets pouvant s'élever au maximum à 6 195 € par an¹²¹. Parmi les indicateurs retenus pour le

versement de cette aide, figure notamment le fait de disposer d'un logiciel métier avec un logiciel d'aide à la prescription (LAP) certifié par la HAS et compatible avec l'usage du dossier médical partagé (DMP). Si cet indicateur n'est pas rempli, le professionnel de santé ne peut toucher le premier volet de l'aide (qui requiert d'atteindre cinq indicateurs cumulatifs), qui s'élevait pour 2020 à 1 960 €¹²². Au-delà de l'équipement, ce « forfait structure » prend en compte l'usage des différents outils dits de « santé numérique », par exemple le pourcentage de feuilles de soins ou d'arrêts maladie traités de façon dématérialisée.

Enfin, conformément à l'article L-1111-8 du Code de la santé publique, et ce afin de garantir au maximum la sécurité des données de santé, « toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même » doit être agréée ou certifiée à cet effet. Plus précisément, ces acteurs intermédiaires, qui peuvent par exemple sous-traiter l'hébergement de données de santé pour le compte d'un hôpital, sont tenus d'héberger ces dernières sur des serveurs certifiés (nouvelle procédure) ou agréés (ancienne procédure) « hébergeurs de données de santé » (HDS)¹²³. Le bilan d'avancement 2020 de la feuille de route stratégique du numérique en santé fait état de 125 hébergeurs HDS validés par l'ANS. Bien que certains établissements de santé soient eux-mêmes certifiés ou agréés HDS (ex. AP-HP, AP-HM, CH de Thuir, CHU de Nantes, CHU de Nîmes), ce n'est pas la norme. Les établissements de santé, groupements hospitaliers territoriaux (GHT), laboratoires d'analyse et autres organismes susceptibles de produire ou recueillir des données de santé ne sont pas soumis à cette obligation s'ils hébergent ces données pour leur propre compte. Au vu de la multiplication des cyberattaques à l'encontre des systèmes d'information (SI) des établissements de santé ces derniers mois, cette absence d'obligation peut soulever des interrogations. Bien entendu, le risque zéro n'existe pas et la cybersécurité en matière de données de santé, comme dans tout autre secteur, ne relève pas uniquement de dispositifs technologiques. Les failles se trouvent bien souvent « entre la chaise et l'écran », et la sécurité des systèmes d'information en santé s'assure au quotidien. Une certification HDS, couplée au respect

121 Voir : <https://www.ameli.fr/paris/medecin/exercice-liberal/vie-cabinet/aides-financieres/modernisation-cabinet>

122 CNAM, *Guide Méthodologique, Forfait structure 2020*, Convention médicale du 25 août 2016, 28 pp. : <https://www.ameli.fr/sites/default/files/Documents/489483/document/note-methodo-forfait-structure-2020.pdf>

123 Voir : <https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante>

de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S)¹²⁴, contribuent toutefois à une forte élévation du niveau de sécurité des SI en santé. Si une prise de conscience des pouvoirs publics commence à poindre à cet égard, celle-ci a, pour l'heure, une portée limitée. Parmi les mesures du plan visant à renforcer la sécurité des réseaux informatiques des établissements de santé, nous pouvons citer le fait qu'« *aucun projet ne pourra désormais faire l'objet d'un soutien de la part de l'État si une part de 5 à 10 % de son budget informatique n'est pas dédiée à la cybersécurité* »¹²⁵. Or, au-delà des seuils budgétaires alloués à la cybersécurité, il convient de penser la façon dont l'adoption du statut HDS peut être encouragée et accompagnée. Lors de leur allocution, les deux ministres ont souligné que ce sont les Agences régionales de santé (ARS) qui seront chargées d'assister les établissements dans leur mise en conformité aux nouvelles obligations de cybersécurité¹²⁶. Renaissance Numérique préconise d'aller plus loin, et d'imposer aux établissements de santé et GHT l'obligation d'être certifiés HDS ou de faire appel à des hébergeurs certifiés HDS. La nécessité d'aligner la certification en matière de cybersécurité sur le standard HDS est d'autant plus critique compte tenu de la volonté des autorités de développer l'interopérabilité. Cette interopérabilité ne pourra, en effet, se développer que si un même niveau de sécurité est garanti entre les services qui doivent échanger des données de santé entre eux. À titre d'exemple, imaginons qu'un médecin utilise un outil « X » (certifié HDS) et décide d'en extraire un rapport qu'il télécharge dans un autre outil (non certifié HDS). Cela reviendrait à compromettre les efforts réalisés par le service « X » puisque, *in fine*, les données se retrouvent dans un espace non certifié HDS. Il est donc urgent que l'ensemble des acteurs, y compris les établissements de santé, se mettent en conformité en s'alignant sur la certification HDS.

Petit à petit, les différents référentiels développés par l'ANS devraient ainsi être massivement adoptés. Mais il ne s'agit pas de simplement « laisser du

temps au temps ». Le respect de ces derniers ne doit pas être une simple « bonne pratique ». Si tous ces référentiels ont vocation à devenir opposables juridiquement, il arrive que certains soient seulement recommandés (lorsqu'un arrêté ne les a pas rendus opposables). Dans ces cas de figure, il convient de maintenir, voire intensifier, les incitations visant la mise en conformité des différents acteurs concernés.

ÉVOLUER VERS UN CADRE À LA FOIS PLUS PROTECTEUR ET PROPICE À L'INNOVATION EN SANTÉ

METTRE EN PLACE UNE RÉGULATION PLUS AGILE

Du fait de leur sensibilité, les données de santé font l'objet d'un régime juridique particulièrement strict. En France, certaines dispositions nationales viennent s'ajouter au cadre européen (RGPD) et entraînent une sécurité juridique renforcée. Ainsi, si le RGPD prévoit un allègement des formalités préalables aux autorisations de traitement de données (en responsabilisant le responsable du traitement, à qui revient la tâche de prouver que son usage des données est conforme au règlement), cette possibilité se voit limitée par la Loi Informatique et Libertés. Conformément à l'article 66 du texte, la procédure allégée ne peut s'appliquer aux traitements de données à des fins de recherche (l'une des exceptions mentionnées à l'article 9 du RGPD). Elle ne s'applique pas non plus aux traitements présentant une finalité d'intérêt public. En revanche, lorsque la base légale du traitement est le consentement, par exemple, la procédure allégée d'autorisation peut s'appliquer. Pour que le traitement soit licite, le responsable de traitement devra néanmoins mettre en place un registre des traitements, mener des analyses d'impact, veiller à encadrer l'information des personnes concernées, formaliser ses rôles et responsabilités, désigner un délégué à la protection des données (dans les cas où cela est obligatoire) et renseigner les actions menées pour garantir la sécurité des données¹²⁷.

Malgré la publication par la CNIL de plusieurs fiches pratiques (sur les registres de traitement, les analyses d'impact, l'information des personnes, le

124 Depuis 2012, la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) fixe les exigences de sécurité des services numériques en santé. Élaborée par la délégation à la stratégie des systèmes d'information de santé (DSSIS) avec l'appui de l'Agence du numérique en santé (ANS), elle rassemble des référentiels d'exigences, des guides de bonnes pratiques et propose un cadre commun de niveau de sécurité des SI du secteur de la santé.

125 Ministère des Solidarités et de la Santé, « Sécurité des réseaux informatiques des établissements de santé : le Gouvernement renforce sa stratégie », Communiqué de presse, 22 février 2021 : <https://solidarites-sante.gouv.fr/actualites/presse/communiqués-de-presse/article/securite-des-reseaux-informatiques-des-etablissements-de-sante>

126 Pour ce qui est de la mise en conformité des acteurs du secteur médico-social, les modalités étaient en cours d'élaboration par le ministère des Solidarités et de la Santé lors de la rédaction du présent rapport.

127 CNIL, « Quelles formalités pour les traitements de données de santé à caractère personnel ? » : <https://www.cnil.fr/fr/quelles-formalites-pour-les-traitements-de-donnees-de-sante-caractere-personnel>

recours à des sous-traitants, etc.), il ressort de la série d'auditions réalisée dans le cadre de ce rapport que le cadre juridique afférent aux traitements de données de santé reste difficile à interpréter. En particulier, ses multiples niveaux de lecture conduiraient certains porteurs de projets à ne pas le respecter à la lettre, ce qui, *in fine*, peut mener certains d'entre eux à renoncer à leurs projets ou à les reporter. Ce non-respect du cadre juridique peut également entraîner des conséquences néfastes du point de vue de la protection des données des citoyens. D'aucuns appellent ainsi de leurs vœux une clarification de l'interprétation du RGPD et de ce qui rentre ou pas dans l'ensemble des exceptions qu'il propose. Le 16 mars 2021, la commission Libertés civiles (Libe) du Parlement européen a adopté sa résolution sur les deux ans d'application du RGPD¹²⁸. Dans cette dernière, les députés demandent notamment aux autorités de protection des données européennes et au Comité européen de la protection des données (l'EDPB) de produire des orientations claires quant à une mise en œuvre appropriée du RGPD dans les politiques de santé publique. Le groupe demande aussi à ce que l'application du règlement par les PME soit facilitée. Afin de concilier protection des individus et innovation, une clarification de l'interprétation qu'il convient de faire du cadre juridique entourant les traitements de données de santé apparaît donc nécessaire.

En particulier, certains porteurs de projets ont le sentiment que, tel qu'interprété actuellement, ce cadre légal leur impose de savoir à l'avance ce qu'ils vont chercher et ce qu'ils vont trouver. Si nous prenons l'exemple des traitements de données de santé à des fins de recherche, pour chaque demande qu'elle reçoit, la CNIL analyse la « *nécessité de recourir à des données à caractère personnel* » et « *la pertinence du traitement au regard de sa finalité déclarée* ». Deux aspects qu'il peut être difficile à anticiper. De même, identifier de façon exhaustive tous les risques susceptibles de se manifester durant le déroulement de la recherche paraît particulièrement complexe. Certains dangers apparaissent aussi en cours de route, sans qu'il ne soit possible de les anticiper. Afin d'encourager l'innovation tout en maintenant un très haut niveau de protection des individus et de leurs données, Renaissance Numérique encourage la mise en place de bacs à sable réglementaires pour les projets de recherche nécessitant le traitement de données personnelles liées à la santé. Cette démarche pourrait permettre aux porteurs de projets

128 « Civil Liberties Committee calls for further improvements to the GDPR implementation and strengthened enforcement », Actualité Parlement européen, Communiqué de presse, 16 mars 2021 : <https://www.europarl.europa.eu/news/fr/press-room/20210311IPR99708/civil-liberties-committee-on-the-gdpr-implementation-and-enforcement>

de mener à bien leur recherche par le biais de mécanismes auditables, et ce sous le contrôle constant des régulateurs. Afin d'assurer une protection maximale des données traitées et la conformité du projet au RGPD, un tel mécanisme nécessiterait que les régulateurs impliqués soient en mesure de contrôler de façon régulière comment la recherche est menée, ce qui sous-entend une totale transparence du processus. S'ils sont utilisés dans certains pays européens comme l'Allemagne et le Royaume-Uni, les bacs à sable réglementaires n'ont jamais fait l'objet d'un véritable débat public en France. Le 15 février 2021, la CNIL a annoncé la création d'un « bac à sable RGPD pour accompagner des projets innovants dans le domaine de la santé numérique »¹²⁹. Destinée à faciliter l'innovation en santé, cette initiative vise à « *retenir des dossiers permettant de mettre en lumière ou d'établir des bonnes pratiques sectorielles (résolution d'une question juridique nouvelle ou importante ou définition de choix techniques, permettant de préciser la doctrine de la CNIL)* »¹³⁰. Or, l'enjeu serait plutôt de donner aux porteurs de projets la latitude nécessaire à la conduite de leur recherche (y compris en levant certaines obligations, dans le cadre du bac à sable), tout en respectant les règles de protection des données personnelles. Les bénéfices de la mise en place d'un bac à sable réglementaire resteront limités si ce dernier ne permet pas cette marge de manœuvre.

DÉPASSER LA BARRIÈRE CULTURELLE POUR TIRER PROFIT DES DONNÉES DE VIE RÉELLE

En lien avec l'innovation dans le domaine de la santé, il est des données qui pourraient être davantage mobilisées et qui le sont, pour l'heure, trop peu en France : les données dites « de vie réelle ». Cette catégorie comprend les données qui ne sont pas collectées dans un cadre expérimental, mais qui sont générées dans la pratique courante, notamment à l'occasion des soins réalisés en routine, mais également en dehors des soins. Ces données sont généralement recueillies par des dispositifs médicaux (DM) ou par des objets connectés et autres applications numériques. Dans un rapport publié en mai 2017, réalisé à la demande de la ministre de la Santé, Marisol Touraine, Bernard Bégaud, Dominique Polton et Franck von Lennep soulignaient déjà le fait que les données de vie réelle représentaient « *des enjeux majeurs de qualité des soins, d'efficacité du système et de régulation*

129 CNIL, « Un « bac à sable » RGPD pour accompagner des projets innovants dans le domaine de la santé numérique », 15 février 2021 : <https://www.cnil.fr/fr/un-bac-sable-rgpd-pour-accompagner-des-projets-innovants-dans-le-domaine-de-la-sante-numerique>

130 *Ibid.*

intelligente », mais que le France ne prenait pas « la mesure de l'enjeu »¹³¹.

Or, une mobilisation plus importante des données de vie réelle permettrait d'aboutir à des logiques de financement et de remboursement des traitements et dispositifs médicaux plus efficaces. Pour ce qui est du remboursement des médicaments par l'Assurance Maladie, par exemple, celui-ci dépend pour l'heure du niveau du « service médical rendu » (SMR) tel que défini par la Haute Autorité de Santé (HAS) lors de l'évaluation de chaque médicament¹³². Le SMR peut ainsi être de niveau « majeur ou important » (auquel cas le médicament est remboursé à hauteur de 65 % par l'Assurance Maladie), « modéré ou faible » (auquel cas le médicament est pris en charge par l'Assurance Maladie à hauteur de 30 %) ou « insuffisant » (dans ce cas, le médicament n'est pas pris en charge). Les médicaments reconnus comme étant irremplaçables et particulièrement coûteux (ex. ceux qui interviennent dans le traitement des affections longue durée, le Sida/VIH ou les cancers) sont, eux, pris en charge à 100 % par l'Assurance Maladie¹³³. En l'absence de disponibilité de données issues d'essais cliniques¹³⁴ randomisés¹³⁵, au lieu d'un avis défavorable au remboursement, la HAS pourrait, par exemple, faire plus souvent appel aux données de vie réelle, pour conditionner une prise en charge ponctuelle et dérogatoire, à la fourniture par l'industriel de données en vie réelle démontrant l'intérêt clinique et l'efficacité du médicament ou du dispositif. Une telle démarche permettrait de conditionner le remboursement des traitements et dispositifs médicaux à leur efficacité telle qu'observée dans la « vie réelle ». Le dernier rapport « Charges et produits » de l'Assurance Maladie préconise particulièrement de suivre cette voie pour les dispositifs médicaux connectés, soulignant que « l'incertitude engendrée par ces dispositifs suggère l'importance d'une approche plus souple prenant en

compte l'efficacité du dispositif tout au long de son cycle de vie »¹³⁶. S'il arrive que la HAS donne des avis conditionnels assortis d'études post-inscriptions (EPI) dans le cadre du renouvellement du remboursement des dispositifs au bout de trois à cinq ans, cela est pour l'heure rarement le cas lors des primo-inscriptions. Des annonces récentes de la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS) de la HAS laissent toutefois penser que l'autorité s'oriente petit à petit vers une utilisation accrue des données de vie réelle dans ses évaluations.

Par ailleurs, l'analyse de l'efficacité des soins se base aujourd'hui essentiellement sur des mesures réalisées hors-contexte (à l'hôpital ou dans un cabinet médical), et sur des mesures fondées sur l'auto-déclaration des patients sur les mois passés. Or, lorsque le médecin pose des questions à son patient sur les derniers mois, ce dernier n'est souvent pas en mesure de donner un résumé détaillé qui soit pertinent, ce qui est normal. De la même façon, un cardiologue, par exemple, n'a pas besoin d'une mesure du rythme cardiaque à un instant T, mais de plusieurs mesures dans des conditions « normales » (c'est-à-dire dans la vie quotidienne, hors de l'hôpital où les mesures peuvent par ailleurs être biaisées par le stress de l'exercice). Si, en plus des mesures réalisées en hôpital ou en cabinet médical à un instant T, il était possible de se baser sur des mesures régulières (par exemple, une fois par semaine au lieu d'une fois par an), l'analyse de l'efficacité des soins prendrait une nouvelle dimension.

Ces données pourraient par ailleurs se montrer très utiles à des fins de prévention, par exemple via le repérage de signaux faibles permettant au corps médical d'agir en amont d'une phase aiguë d'une maladie. Pour l'heure, il semblerait qu'une plus grande utilisation des données de vie réelle dans les parcours de soins se heurte à un problème d'acceptabilité, à la fois des professionnels de santé (qui ne sont pas tous sensibilisés à ces enjeux) et des patients (pour qui les démarches ne sont pas toujours suffisamment transparentes).

La question du recours aux données de vie réelle se pose également en matière d'évaluation des traitements et dispositifs médicaux lors de leur

131 Bernard Bégaud, Dominique Polton, Franck von Lennep, *Les données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé. L'exemple du médicament*, mai 2017 : https://solidarites-sante.gouv.fr/IMG/pdf/rapport_donnees_de_vie_reelle_medicaments_mai_2017vf.pdf

132 Haute Autorité de Santé, « Le service médical rendu (SMR) et l'amélioration du service médical rendu (ASMR) », 16 avril 2013 : https://www.has-sante.fr/jcms/r_1506267/fr/le-service-medical-rendu-smr-et-l-amelioration-du-service-medical-rendu-asmr

133 Assurance Maladie, « Tableaux récapitulatifs des taux de remboursement », 6 janvier 2021 : <https://www.ameli.fr/paris/assure/remboursements/rembourse/tableau-recapitulatif-taux-remboursement/tableau-recapitulatif-taux-remboursement>

134 Un essai clinique, ou étude clinique, ou encore essai thérapeutique, est une étude scientifique réalisée en thérapeutique médicale humaine pour évaluer l'efficacité et la tolérance d'une méthode diagnostique ou d'un traitement. En fonction du type d'étude et du stade du développement du médicament, les investigateurs enrôlent des volontaires sains ou des patients.

135 Voir : Wikipédia, « Étude randomisée en double aveugle » : https://fr.wikipedia.org/wiki/%C3%89tude_randomis%C3%A9e_en_double_aveugle#:~:text=L%27%C3%A9tude%20randomis%C3%A9e%20en%20double,que%20la%20physique%20et%20la

136 Assurance Maladie, « Améliorer la qualité du système de santé et maîtriser les dépenses - Propositions de l'Assurance Maladie pour 2021 », Rapport au ministre chargé de la Sécurité sociale et au Parlement sur l'évolution des charges et des produits de l'Assurance Maladie au titre de 2021 (loi du 13 août 2004), juillet 2020, p. 211 : https://assurance-maladie.ameli.fr/sites/default/files/2020-07_rapport-propositions-pour-2021_assurance-maladie_1.pdf

mise sur le marché. Comme évoqué précédemment (voir la section « Un écosystème difficile à appréhender dans sa globalité »), la commercialisation des dispositifs médicaux (DM) obéit à des règles strictes. Il en est de même pour les médicaments. En France, c'est la Haute autorité de santé (HAS) qui est chargée d'évaluer les médicaments et dispositifs médicaux susceptibles de faire l'objet d'un remboursement individualisé. Afin d'obtenir un avis favorable, les industriels à l'origine d'éventuels produits de santé innovants doivent notamment fournir des données issues d'essais cliniques randomisés pour prouver l'efficacité de leur solution. Alors qu'elles portent sur des cohortes relativement limitées au niveau du nombre de patients (généralement, quelques centaines de personnes), mais également dans le temps (3-6 mois), les études cliniques randomisées restent la norme. Les données de vie réelle, quant à elles, récoltées par le biais de dispositifs médicaux connectés ou d'applications dédiées, concernent parfois plusieurs centaines de milliers de personnes, voire des millions. Or, il ressort des auditions menées dans le cadre de cette étude que les industriels qui intègrent des données de vie réelle dans leurs dossiers d'évaluation auprès de la HAS, ont parfois le sentiment que ces données ne sont pas suffisamment considérées comme étant de même qualité que des données issues d'études randomisées.

Si la question n'est pas de savoir si les données de vie réelle peuvent se substituer aux données issues d'études cliniques, il convient toutefois de s'interroger sur leur éventuelle complémentarité. Plutôt que de les opposer, et de les réserver chacune à des usages distincts, il convient de considérer que chacune a ses limites et ses vertus. D'où proviennent alors les blocages, les réticences quant à une utilisation plus systématique des données de vie réelle dans l'évaluation des médicaments et dispositifs médicaux ? Existe-t-il des freins juridiques à leur utilisation ? Des freins techniques ?

Il semblerait que la réponse soit un mélange d'obstacles techniques et culturels, les limites ne se situant pas, de fait, au niveau juridique. Quelques obstacles subsistent encore en effet du point de vue technique, notamment en termes d'interopérabilité des données. Par ailleurs, certains acteurs questionnent la qualité et la fiabilité des données de vie réelle, quand d'autres s'interrogent sur la capacité des essais cliniques randomisés à répondre à ces questions. Une autre raison qui est souvent revenue lors des auditions menées dans le cadre de ce rapport est la persistance de freins culturels, qui seraient en partie issus de la doctrine du régulateur français. Certains pays européens, à l'instar de la Belgique, de l'Espagne ou

du Royaume-Uni, leur accordent une place plus importante. Comme évoqué dans les dernières communications de la CNEDiMTS¹³⁷, la HAS travaille toutefois à l'élaboration d'un guide méthodologique sur les études prises en compte dans les évaluations de dispositifs médicaux et de technologies de santé. Ce guide, qui a vocation à être partagé avec les représentants des industriels concernés, vise à expliciter les principes d'évaluation de la commission. Cette initiative devrait permettre de réaffirmer la doctrine de la CNEDiMTS concernant la prise en compte des données de vie réelle, et ainsi clarifier cette question pour certains acteurs de la chaîne, en particulier les fabricants de DM. Les dispositifs médicaux et les technologies de santé ne constituent toutefois qu'une partie de l'offre de santé évaluée par la HAS. Qu'en est-il, par exemple, de l'utilisation de données de vie réelle dans le cadre de l'évaluation des médicaments ? Afin de dépasser le relatif flou actuel, **Renaissance Numérique appelle les acteurs concernés à placer la question de l'utilisation des données de vie réelle au cœur du débat public.** Pour ce qui est de leur utilisation à des fins d'évaluation des médicaments et dispositifs médicaux, il serait en outre utile que la HAS **formalise sa doctrine en la matière.** Concernant le premier point, il convient de noter que le Conseil général de l'économie, dans sa consultation publique « Structuration de la Filière e-santé », a introduit un volet intitulé « Circulation maîtrisée des données, IA et recherche », dans lequel il est proposé de « *permettre une exploitation plus large des données de vie réelle dans le respect du RGPD* »¹³⁸.

Il apparaît indispensable que les éléments susmentionnés soient pris en compte dans le projet de création d'une Agence de l'innovation en santé récemment annoncé par le ministère des Solidarités et de la Santé.

METTRE LE CITOYEN AU CŒUR DE LA GOUVERNANCE DES DONNÉES DE SANTÉ

Redéfinir la gouvernance des données de santé doit être l'opportunité de mettre le citoyen au cœur du processus. L'exploitation grandissante des données de santé

¹³⁷ Voir notamment l'ordre du jour de la réunion du Collège délibératif de la HAS du 10 juin 2021 : https://www.has-sante.fr/upload/docs/application/pdf/2021-06/2021_06_04_odj_cd_2021_06_10_vd_signe.pdf

¹³⁸ Conseil Général de l'Économie, Enquête en ligne - Structuration de la Filière e-santé : https://forms.office.com/Pages/ResponsePage.aspx?id=00mEUDLWm0KXzvitrOn55_p8Ud_bjFPu7kQtf-HA8hIUQTlOTVI2TVdCSUNSuk9XN0Y0OTRDQTNFOC4u

dans les parcours de soins et à des fins de recherche concerne l'ensemble de la population, les jeunes comme les moins jeunes, les personnes atteintes de pathologie comme celles en bonne santé. Or, les associations de patients sont très souvent reconnues comme seules entités représentatives de la population possédant une légitimité suffisante pour être entendues au sein des instances sanitaires. Au-delà des patients et des associations de patients, c'est donc plus largement aux citoyens dans leur ensemble qu'il convient d'accorder un plus grand rôle dans l'élaboration et la mise en œuvre de la politique de santé publique.

VERS UNE PLUS GRANDE TRANSPARENCE ET UNE MEILLEURE PRISE EN COMPTE DES ATTENTES DES CITOYENS EN MATIÈRE DE SANTÉ PUBLIQUE

Comme évoqué dans le rapport de la « mission Bothorel » rendu public en décembre 2020, « *la donnée est un moyen d'évaluer correctement nos politiques publiques. D'une part, faire de la « data », ce n'est jamais que fiabiliser et permettre en temps réel le bon vieux contrôle de gestion ; et c'est aussi se donner enfin les moyens de suivre l'exécution des dépenses publiques.* »¹³⁹ Pour le moment, cette culture peine à s'installer dans l'administration française. Afin d'encourager un changement de pratique à cet égard, le plan de transformation de l'action publique, qui s'inscrit dans la lignée de la mission précitée, invite l'ensemble des ministères à se saisir de la question de leurs données. Parmi les trois chantiers prioritaires identifiés pour la période 2021/2022, le premier est celui du pilotage et de la gouvernance des données publiques. Plus précisément, il s'agit d'ouvrir les données publiques détenues par les différents ministères, en vue d'améliorer le pilotage des politiques et permettre plus de transparence dans l'action publique. Le plan prévoit en outre que de nouvelles politiques publiques intègrent le baromètre des résultats de l'action publique lancé par le gouvernement en janvier 2021¹⁴⁰. Ainsi, pour un ensemble de trente-six politiques jugées prioritaires, chaque citoyen pourra se renseigner, sur le site du gouvernement, pour savoir où les actions en sont et les objectifs à atteindre d'ici la fin du quinquennat, que ce soit au niveau national ou de chaque département. Cette démarche devrait, *in fine*, permettre de combler

en partie le vide existant en matière de retours d'expérience vis-à-vis des différentes réformes entreprises en matière de santé au niveau national. Pour l'heure, il se révèle en effet extrêmement difficile de qualifier et quantifier précisément les bénéfices apportés par ces dernières aux citoyens et au système de santé dans son ensemble, à la fois au niveau national et dans les territoires.

Il apparaît en outre urgent de faire en sorte que les citoyens puissent prendre part aux débats qui façonnent et fixent les objectifs de la politique de santé publique. Comme précédemment évoqué, la transformation numérique de notre système de santé pose des questions d'ordre éthique, économique, technique et juridique qui relèvent de choix collectifs. Les citoyens doivent être invités à se prononcer sur ces enjeux, et ce d'autant plus que, comme cela a été le cas dans le cadre de la lutte contre la pandémie de Covid-19, certains impératifs de santé publique peuvent venir percuter des libertés individuelles comme la liberté d'aller et venir. Si la politique de santé publique est en grande partie élaborée au sein de l'Assemblée nationale, elle émane toutefois principalement des orientations fixées par la Caisse nationale de l'Assurance Maladie (CNAM) dans ses « Rapport Charges et produits » remis annuellement au gouvernement et au Parlement. Ces derniers consistent en une analyse et des propositions concrètes visant à améliorer la qualité du système de santé et maîtriser ses dépenses¹⁴¹. C'est sur la base de ces rapports que sont élaborés chaque année les projets de loi de financement de la sécurité sociale (PLFSS), qui s'intéressent essentiellement au budget de l'Assurance Maladie. À cette occasion, les citoyens ne sont pas consultés sur leurs attentes concernant le système de santé, et il n'existe à ce jour pas de réel débat portant sur l'orientation globale de la santé publique en France. De récents travaux du Haut conseil pour l'avenir de l'assurance maladie (HCAAM) laissent toutefois entrevoir la possibilité d'avancer vers des démarches incorporant davantage de démocratie sanitaire, avec des PLFSS qui seraient des déclinaisons annuelles des plans d'orientation de la santé publique votés à chaque début de quinquennat¹⁴². Alors que la réforme « Ma Santé 2022 » touche à sa fin, le temps est venu de penser à l'élaboration de la stratégie à adopter sur les quatre à cinq prochaines années. L'occasion doit alors être saisie pour impliquer beaucoup plus largement les citoyens dans ce proces-

139 Gouvernement (Mission Bothorel), *Pour une politique publique de la donnée*, Décembre 2020, p. 7 : https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publique_de_la_donnee_-_23.12.2020_0.pdf

140 Gouvernement, « Lancement du baromètre des résultats de l'action publique », 13 janvier 2021 : <https://www.gouvernement.fr/lancement-du-barometre-des-resultats-de-l-action-publique>

141 Pour en savoir plus, voir : <https://assurance-maladie.ameli.fr/qui-sommes-nous/publications-reference/assurance-maladie/rapports-charges-et-produits/rapport-charges-produits>

142 Voir notamment l'avis du HCAAM sur la régulation du système de santé adopté le 22 avril 2021, 23 pp. : <https://www.securite-sociale.fr/files/live/sites/SSFR/files/medias/HCAAM/2021/HCAAM%20-%20Avis%20regulation%20HCAAM%20avril%202021.pdf>, récemment complété par le Rapport du HCAAM sur la régulation du système de santé adopté le 27 mai 2021, : <https://www.securite-sociale.fr/files/live/sites/SSFR/files/medias/HCAAM/2021/HCAAM%20-%20Rapport%20r%c3%a9gulation%20HCAAM%202021.pdf>

sus, que ce qui n'a été fait dans le passé. À cet égard, au-delà des associations de patients, les associations de consommateurs et d'usagers doivent monter en capacité sur ces sujets afin d'étendre la voix des citoyens dans ces débats.

Une plus grande transparence dans les choix opérés et dans les priorités fixées par certaines instances comme l'Assurance Maladie ou le *Health Data Hub* peut également contribuer à placer la préoccupation citoyenne au cœur des enjeux liés aux données de santé et, *in fine*, renforcer la démocratie sanitaire. Les citoyens pourraient, par exemple, être invités à contribuer à la fixation des priorités de l'Assurance Maladie ou des priorités de recherche des structures comme le *Health Data Hub*. Cela nécessite toutefois que ces acteurs communiquent régulièrement et de façon compréhensible sur les objectifs recherchés, les programmes de recherche en cours, les pathologies ciblées, et les résultats concrets de leurs actions. Cela demande également une certaine proactivité de la part des citoyens, notamment un effort pour accéder à cette information. Afin de compléter ces démarches, il conviendrait ainsi de décliner des dispositifs de concertation reposant sur des logiques de représentation, de façon à ce que la voix des citoyens soit entendue sur des points précis (par exemple, le déploiement de nouveaux services de santé numérique par la puissance publique, etc.). Pour que de telles initiatives portent réellement leurs fruits, une attention particulière doit cependant être accordée aux logiques de décisions qui en découlent, afin d'assurer le respect des attentes formulées par les citoyens et d'éviter tout effet déceptif.

RENFORCER LA REPRÉSENTATION DES CITOYENS DANS LES INSTANCES DE GOUVERNANCE DES DONNÉES DE SANTÉ

Il est également souhaitable que les citoyens soient davantage impliqués et mieux représentés dans certaines instances de gouvernance des données de santé. Parmi les cinquante-six membres fondateurs du *Health Data Hub*, seul un, l'Union nationale des associations agréées d'usagers du système de santé (France Assos Santé)¹⁴³, représente les citoyens. À quelques rares exceptions, à l'instar de l'UFC Que Choisir, du Conseil National des Associations Familiales Laïques et de l'association Consommation Logement Cadre de vie, France Assos Santé est constituée presque exclusivement d'associations de patients.

Ce sont donc essentiellement des citoyens atteints de pathologies qui sont représentés dans les instances du *Health Data Hub*, et au travers d'une seule « voix ». Quid des citoyens en bonne santé ? La convention qui unit les membres fondateurs du hub n'exclut pas de nouvelles adhésions¹⁴⁴. Afin de faire entendre la voix des citoyens dans cette instance, il serait souhaitable dans un avenir proche d'élargir cette représentation et que des associations de la société civile, de défense des droits notamment, y soient intégrées.

POUR UNE PARTICIPATION DIRECTE DES CITOYENS À L'AMÉLIORATION DU SYSTÈME DE SANTÉ VIA LA REMONTÉE DE DONNÉES

Au-delà de ce niveau macro, il convient d'embarquer les citoyens dans les enjeux liés aux données de santé au plus près de leur quotidien. Cela passe notamment par une plus grande information et une plus grande sensibilisation dans le cadre des parcours de soins. Si les bénéfices que peuvent apporter la collecte et l'exploitation des données de santé sont généralement admis par les professionnels du secteur, ils restent pour l'heure peu connus du grand public. Chaque étape du parcours de soins doit alors être une occasion pour les différents acteurs impliqués d'informer ces derniers sur la façon dont leurs données peuvent être utilisées afin d'améliorer le système de santé dans son ensemble, sur leurs droits, et sur les garanties (en termes de sécurité, de confidentialité) qui entourent le partage de ces données. À chaque fois que cela est possible, et s'ils le souhaitent, les citoyens doivent être en mesure de faire remonter leurs données, par exemple afin de contribuer aux programmes de recherche médicale de leur choix ou à l'évaluation des actes médicaux, dans une démarche contributive. Comme déjà évoqué, c'est en effet par la pratique que les citoyens se familiariseront petit à petit avec les enjeux qui sous-tendent les données de santé et leur exploitation.

Cette remontée d'informations terrain permettrait, en outre, de mieux connaître l'impact des politiques de santé publique sur l'ensemble du territoire. Une telle démarche participerait de la régulation du système de santé « par les données » et permettrait de faire participer activement les citoyens à sa gouvernance, dans une logique *bottom-up*. À cet égard, Renaissance Numérique encourage une « plateformes » de la régulation du système de santé. Cela pourrait par exemple passer par la mise en place de remontées

¹⁴³ Gérard Raymond, le Président de France Assos Santé, est par ailleurs vice-président du *Health Data Hub*.

¹⁴⁴ Sous réserve de l'approbation d'une majorité qualifiée des deux-tiers des droits de vote des membres de l'assemblée générale.

d'alertes ou l'envoi de formulaires par le biais de Mon Espace Santé. Des indicateurs universels simples (délais de prise en charge, nombre de séjours hospitaliers, présence ou non d'un service de proximité de qualité, etc.) pourraient être mis en place, sur lesquels les citoyens seraient invités à donner leur avis. En participant ainsi à l'évaluation de la qualité des soins, le citoyen devient acteur de sa prise en charge et contribue à l'amélioration du système dans sa globalité. Si, grâce aux retours d'expériences ainsi accumulés, on se rend compte que, sur tel territoire, pour telle pathologie, les délais d'obtention de rendez-vous sont de deux ans, alors on a identifié un problème, et on peut se donner les moyens de le résoudre. Cette initiative nécessiterait toutefois que les instances qui contribuent à la régulation du numérique en santé, à l'instar de la Haute autorité de santé (HAS), du ministère des Solidarités et de la Santé, de l'Assurance Maladie et des ARS, soient dotées de capacités leur permettant de traiter ces remontées d'informations et de les prendre en compte dans la définition des objectifs de santé publique. La remontée de données à tous les niveaux du système de santé devrait également permettre de faire apparaître des singularités régionales qui pourraient permettre aux instances de gouvernance locales du système (notamment les ARS) de gagner en efficacité.

S'il convient de souligner le travail déjà accompli en vue de clarifier la gouvernance des données de santé, les efforts consentis, notamment par la Délégation du numérique en santé et l'Agence du numérique en santé, en termes de pédagogie, mais également en termes de développement de référentiels socles, doivent être poursuivis et accentués. Alors que différentes initiatives viennent tout juste d'être lancées où le seront très prochainement, il n'est pas trop tard pour s'en donner les moyens et pour placer le citoyen au cœur du système.

CONCLUSION

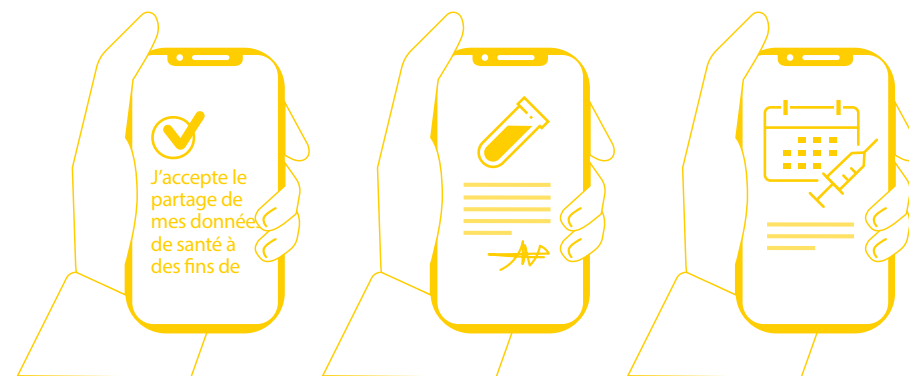
LE CITOYEN, PILIER DE L'ESPACE NUMÉRIQUE DE SANTÉ EUROPÉEN



Nul ne peut ignorer les changements en cours en matière d'exploitation des données au service du système de santé. Impulsé dans le cadre de la stratégie « Ma Santé 2022 », le « virage numérique » en santé, renforcé par la crise du Covid-19, se concrétise un peu plus chaque jour. La période 2020-2021 aura marqué un tournant en la matière, avec une explosion du recours aux téléconsultations¹⁴⁵, le lancement du *Health Data Hub* et la mise en place en phase pilote de « Mon Espace Santé » dans trois départements (la Haute-Garonne, la Loire Atlantique et la Somme). Mais ces changements ne seront réellement bénéfiques que si les citoyens parviennent à s'en saisir. Outre une meilleure application des référentiels techniques existants (en particulier en matière de cybersécurité et d'interopérabilité), ceci nécessite encore de sérieux efforts d'acculturation de tous les acteurs de la chaîne de santé, jusqu'aux citoyens. « Se saisir » des données de santé doit en outre passer par une familiarisation avec ces données au niveau le plus micro possible, au quotidien, notamment dans le cadre des étapes du parcours de soins. *In fine*, ces développements doivent viser non seulement à rendre le système sanitaire plus efficient, mais également à placer le citoyen au cœur du système.

Ce souci de développer des outils utiles et bénéfiques avant tout aux citoyens se retrouve dans l'annonce récente de la Commission européenne concernant sa stratégie pour une identité numérique européenne¹⁴⁶. Le but du futur portefeuille européen d'identité numérique annoncé début juin 2021 : permettre à tout citoyen ou résident de s'identifier numériquement, et de stocker et gérer des données sensibles, y compris des données de santé, et des documents officiels sous forme électronique. S'inscrivant dans le cadre du règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS), cette initiative vise à lutter contre les disparités existant d'un État membre à l'autre en matière d'identité numérique.¹⁴⁷ Dans le même temps, les travaux de l'action conjointe lancée par la Commission européenne afin de définir les contours du futur espace européen des données de santé se poursuivent, avec en ligne de mire une proposition législative et un projet

pilote attendus pour la fin de l'année 2021 ou le début de l'année 2022. Dès lors, si le défi actuel consiste dans un premier temps à se mettre à niveau à l'échelle nationale, la prochaine étape sera de penser la place du citoyen dans l'espace numérique de santé européen. Une démarche qui nécessitera inévitablement un certain degré d'harmonisation entre États membres, ne serait-ce qu'en termes de définitions. Ce qui constitue une équipe de soins n'est, par exemple, pas entendu de la même manière d'un pays à l'autre. Il conviendra alors de faire en sorte que ces disparités ne se transforment pas en obstacles, notamment dans le cadre de l'espace européen des données de santé, qui vise à être accessible à l'ensemble des professionnels de santé des États membres. Dans les développements en cours et à venir, il sera en outre primordial de garder à l'esprit que les données de santé et leur circulation accrue ont une première vocation qui est d'apporter des bénéfices aux citoyens et renforcer leurs droits. Aussi, une attention particulière doit être maintenue à l'égard d'initiatives qui par leur usage de ces données pourraient affaiblir les équilibres fondamentaux au prétexte d'une meilleure santé. L'objectif de santé ne se suffit pas en soi – pas davantage que d'autres objectifs légitimes –, tant qu'on n'examine pas ses modalités de mise en œuvre.



¹⁴⁵ L'Assurance Maladie a pris en charge 12,8 millions de téléconsultations entre janvier et août 2020, contre seulement 138 000 entre septembre 2018 et fin décembre 2019.

¹⁴⁶ Commission européenne, communiqué de presse, « La Commission propose une identité numérique fiable et sécurisée pour tous les Européens », 3 juin 2021 : https://ec.europa.eu/commis-sion/presscorner/detail/fr/ip_21_2663

¹⁴⁷ Pour l'heure, la France ne s'est par exemple pas dotée d'un tel service, même si le dispositif France Connect en constitue les prémices.

LES PRÉCONISATIONS DE RENAISSANCE NUMÉRIQUE



Afin de passer un cap dans l'exploitation des données de santé au service d'une meilleure gouvernance et plus grande efficacité du système de santé, Renaissance Numérique formule onze préconisations autour de trois axes :

ENGAGER DE SÉRIEUX EFFORTS D'ACCULTURATION EN MATIÈRE DE DONNÉES DE SANTÉ, ET PLUS GÉNÉRALEMENT EN MATIÈRE DE NUMÉRIQUE EN SANTÉ

Recommandation n°1 - De sérieux efforts d'acculturation doivent être dirigés vers les acteurs de la chaîne de santé (professionnels de santé, associations de patients, etc.), jusqu'aux citoyens, y compris les nouveaux entrants, dont les acteurs de la *tech* qui investissent le champ de la santé et ne sont pas sensibilisés à tous les enjeux qui le sous-tendent.

Recommandation n°2 - Certains métiers, à l'instar des pharmaciens, des infirmiers ou des médecins, ont vocation à jouer un rôle dans la diffusion de cette culture des données de santé, en devenant des sortes de « médiateurs », tiers de confiance agissant en relai entre les citoyens et les autres acteurs de la chaîne (État, industriels, etc.). Ils doivent être accompagnés et revalorisés en ce sens.

Recommandation n°3 - Les associations de patients, d'usagers et de consommateurs, à condition qu'elles montent en compétences sur le sujet des données de santé, ont également un rôle important à jouer dans cet effort d'acculturation.

Recommandation n°4 - En complément, il convient de massifier la politique de médiation numérique, afin de sensibiliser l'ensemble des citoyens (y compris les moins connectés) aux enjeux liés aux données de santé, et de les accompagner dans leurs usages du numérique en santé.

CLARIFIER LA GOUVERNANCE DES DONNÉES DE SANTÉ

Recommandation n°5 - Clarifier la gouvernance des données de santé nécessite de clarifier les rôles et de renforcer la collaboration entre les différents acteurs impliqués dans le pilotage de la politique publique des données de santé.

Recommandation n°6 - Il convient en outre d'inciter les différents acteurs de la chaîne de santé au plus grand partage de leurs données. Des outils et mécanismes incitatifs (*data trusts*, solutions contractuelles, outils techniques) existent et doivent être plus largement activés.

Recommandation n°7 - Clarifier la gouvernance des données de santé passera également par une meilleure application des exigences liées aux référentiels techniques d'interopérabilité et de sécurité : inciter les acteurs à adopter les référentiels édictés par l'ANS (cadre d'interopérabilité SIS, utilisation de l'outil Convergence, etc.) et imposer aux hôpitaux et GHT l'obligation d'être certifiés HDS ou de recourir à des services certifiés HDS.

Recommandation n°8 - Enfin, il convient d'évoluer vers un cadre à la fois protecteur et plus propice à l'innovation en santé : mise en place de bacs à sable réglementaires, mobilisation accrue des données de vie réelle.

METTRE LE CITOYEN AU CŒUR DE LA GOUVERNANCE DES DONNÉES DE SANTÉ

Recommandation n°9 - Mettre les citoyens au cœur du système de santé nécessite qu'ils puissent prendre davantage part aux arbitrages collectifs sur lesquels il convient de trancher en matière de données de santé, en étant consultés sur les plans d'orientation de la santé publique et via des démarches de concertation portant sur des points spécifiques.

Recommandation n°10 - Les citoyens doivent également être mieux représentés dans certaines instances de gouvernance des données de santé (Assurance Maladie, *Health Data Hub*), par le biais des associations de patients, de consommateurs, d'usagers et de défense des droits.

Recommandation n°11 - Ils doivent enfin être mis en capacité de faire remonter directement leurs données à des fins d'évaluation de la qualité des soins et de régulation du système de santé par les données, et ainsi participer activement à l'amélioration du système de santé.

GLOSSAIRE

NOTIONS CLÉS

Anonymisation : traitement de données qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit, de manière irréversible.

Appariement : rapprochement d'ensembles de données distincts, à l'aide d'informations communes (par exemple, regroupement des données patient issues de différentes sources).

Démocratie sanitaire : le concept de démocratie sanitaire vise à associer l'ensemble des acteurs de santé pour élaborer et mettre en œuvre la politique de santé, dans un esprit de dialogue et de concertation. Il est sanctuarisé dans le titre III de la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

Données de vie réelle : les données qui ne sont pas collectées dans un cadre expérimental, mais qui sont générées dans la pratique courante, notamment à l'occasion des soins réalisés en routine. Ces données sont généralement recueillies par des dispositifs médicaux (DM) ou par des objets connectés et autres applications numériques.

Données de santé : les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

Données de santé par nature : les données qui sont intrinsèquement et de manière évidente des données de santé.

Données de santé par croisement : les données qui, prises indépendamment, ne constituent pas des données de santé, mais qui, lorsqu'elles sont croisées avec d'autres, peuvent donner une indication sur l'état de santé ou le risque pour la santé d'une personne.

Données de santé par destination : les données qui deviennent des données de santé en raison de leur utilisation à des fins médicales.

Données médicales : les informations collectées et détenues par les professionnels de santé. Ces dernières sont recueillies dès la naissance (poids, taille, compte-rendu médical), puis tout au long de la vie lors de visites dans les lieux de soins et les pharmacies.

Dossier médical partagé (DMP) : le DMP est un carnet de santé numérique qui conserve et sécurise les informations de santé (traitements, résultats d'exams, allergies, etc.) des usagers du système de santé français. Il permet de partager ces informations avec les professionnels de santé en toute sécurité. À partir du 1^{er} janvier 2022, son accès se fera via « Mon Espace Santé », dont il deviendra une des briques.

Mon Espace Santé : Mon Espace Santé est un espace numérique de santé (ENS), un « portail patient » qui sera accessible à tout usager du système de santé français à partir du 1^{er} janvier 2022. Ce dernier vise à permettre un accès facilité et sécurisé à un certain nombre de services : DMP, messagerie sécurisée, « agenda-santé » permettant de consolider les différents événements de santé et le « store ENS », un catalogue de services de santé numériques référencés par la puissance publique.

Interopérabilité : la capacité d'un système informatique à communiquer, exécuter des programmes ou transférer des données avec d'autres produits ou systèmes informatiques, existants ou futurs, sans contrainte pour l'utilisateur dans l'accès ou la mise en œuvre, et sans multiplier les efforts de développements¹⁴⁸.

¹⁴⁸ <https://www.houdart.org/les-entrepots-hospitaliers-de-donnees-du-mythe-a-la-realite/>

Pseudonymisation : traitement (réversible) de données à caractère personnel qui permet de rendre impossible toute identification de la personne concernée sans avoir recours à des informations supplémentaires, pourvu que ces informations supplémentaires soient conservées séparément et soumises à des mesures de protection.

Système national des données de santé (SNDS) : géré par l'Assurance Maladie, le SNDS constitue une base de données complète et détaillée sur le parcours des patients et l'organisation du système de soins sur le territoire français. Il rassemble :

- Le Système national d'information interrégimes de l'Assurance Maladie (SNIIRAM) : un entrepôt de données anonymes regroupant les informations issues des remboursements effectués par l'ensemble des régimes d'assurance maladie pour les soins du secteur libéral.
- Les données issues du Programme de médicalisation des systèmes d'information (PMSI) : les données des hôpitaux et autres établissements de santé.
- Le CépiDC : une base gérée par l'Inserm qui rassemble les données sur les causes médicales de décès pour l'ensemble de la population.

ACTEURS CLÉS

Agence du numérique en santé (ANS) : anciennement Agence des systèmes d'information partagés de santé ou ASIP-Santé, l'ANS est une agence gouvernementale française chargée de la santé numérique. Elle élabore notamment les référentiels éthiques, de sécurité et d'interopérabilité afférents aux données de santé.

Agence régionale de santé (ARS) : établissement public administratif de l'État français chargé de la mise en œuvre de la politique de santé dans sa région.

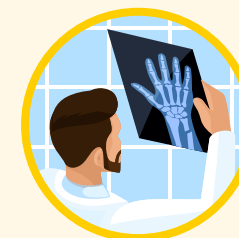
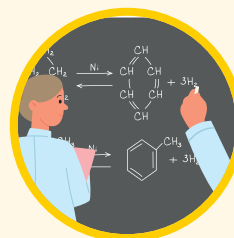
Caisse nationale d'Assurance Maladie des travailleurs salariés (CNAMTS) : la CNAMTS pilote les 128 caisses primaires d'assurance maladie (CPAM) implantées au niveau local chargées de verser les prestations d'assurance maladie de la sécurité sociale. Elle est le gestionnaire historique du Système national des données de santé (SNDS).

Délégation ministérielle du numérique en santé (DNS) : la DNS assure le pilotage de l'ensemble des chantiers de transformation du numérique en santé en France. Elle est rattachée directement au ministre des Solidarités et de la Santé et assure un pilotage resserré de l'Agence du numérique en santé (ANS).

Direction de la recherche, des études, de l'évaluation et des statistiques (DREES) : rattachée au ministère des Solidarités et de la Santé, la DREES est le service statistique public du ministère. Elle fait partie du service statistique public piloté par l'INSEE.

Haute autorité de santé (HAS) : la HAS est une autorité publique indépendante qui contribue à la régulation du système de santé par la qualité. Elle exerce ses missions dans les champs de l'évaluation des produits de santé (médicaments et dispositifs médicaux), des pratiques professionnelles, de l'organisation des soins et de la santé publique.

Institut national de la santé et de la recherche médicale (INSERM) : établissement public à caractère scientifique et technologique français spécialisé dans la recherche médicale.



REMERCIEMENTS

Nous remercions pour leur contribution, les différents acteurs qui ont participé aux auditions, à savoir :

Isabelle Adenot, Présidente de la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS), Haute autorité de santé (HAS)

Charles-Pierre Astolfi, Directeur du projet « Systèmes d'information vaccination », Ministère des Solidarités et de la Santé

Nesrine Benyahia, Co-présidente du collège numérique, Société Française de Santé Digitale

Éric Bothorel, Député des Côtes d'Armor, chargé par le gouvernement de la mission sur l'ouverture des données et des codes sources

Éric Chenut, Vice-président, MGEN

Cécile Chevance, Directrice du pôle Finance/FHF Data, Fédération Hospitalière de France (FHF)

Olivier Clatz, Directeur du Grand Défi « Amélioration des diagnostics médicaux par l'intelligence artificielle », Secrétariat général pour l'investissement - Conseil de l'Innovation, Services du Premier Ministre

Stéphanie Combes, Directrice, *Health Data Hub*

Elisabeth Doineau, Sénatrice de la Mayenne

Etienne Drouard, Avocat associé, Hogan Lovells

Philippe Emery, Président, Abbott France

Claude Gissot, Directeur des études et des statistiques, CNAM

David Gruson, Co-président du collège numérique, Société Française de Santé Digitale

Caroline Guillot, Directrice adjointe des relations associations et citoyens, *Health Data Hub*

Hélène Guimiot-Bréaud, Cheffe du service Santé, CNIL

Cyrille Isaac-Sibille, Député du Rhône, Rapporteur sur le DMP et les données de santé

Aurora Ursula Joala, Conseillère « Développement des services électroniques et politique d'innovation », Ministère estonien des Affaires sociales

Irina Kalderon-Libal, Responsable des politiques, Unité « Santé en ligne, bien-être et vieillissement », DG CNECT, Commission européenne

Kalle Killar, Secrétaire général adjoint « Développement des services électroniques et politique d'innovation », Ministère estonien des Affaires sociales

Jean-Christophe Klein, Co-fondateur et CEO, Libhéros

Christine Laliberté, Présidente, Association des Infirmières Praticiennes Spécialisées du Québec (AIPSQ)

Yann-Mael Le Douarin, Conseiller médical télésanté, DGOS, Ministère des Solidarités et de la Santé

Franck Lethimonnier, Directeur de l'institut thématique « Technologies pour la santé », Institut national de la santé et de la recherche médicale (INSERM)

Isabelle Levasseur, Vice-présidente, Association des Infirmières Praticiennes Spécialisées du Québec (AIPSQ)

Jacques Lucas, Président, Agence du numérique en santé (ANS)

Jelena Malinina, Digital Health Policy Officer, Bureau européen des unions de consommateurs (BEUC)

Bernard Ourghanlian, Directeur Technique et Sécurité, Microsoft France

Antoine Piau, Médecin en gériatrie et porte-parole de l'unité médicale transversale de télésanté (UMTT), CHU Toulouse

Stéphane Pierrefitte, Directeur de l'innovation et des systèmes d'information, GHU de Paris psychiatrie et neurosciences

Jean-Marc Pinguet, Directeur de la médecine personnalisée, Roche

Dominique Pon, Directeur général de la Clinique Pasteur de Toulouse, Responsable stratégique de la transformation numérique en santé, Ministère des Solidarités et de la Santé

Noemi Porrello, Responsable « Données de vie réelle », Direction de la gestion des accès intégrés, Roche Italie

Didier Quercioli, Délégué national et Président de MGEN Technologies, MGEN

Gérard Raymond, Président, France Assos Santé et Vice-président, *Health Data Hub*

Dario Scapola, Directeur de la gestion des accès intégrés, Roche Italie

Valérie Schlosser, Directrice Données et Stratégie numérique, Groupe Vvy

Chloé Simpson, Responsable du projet « Impact DATA », Croix-Rouge (21)

Juliette Valains, Responsable Transformation Digitale, Croix-Rouge

Guy Vallancien, Chirurgien, Universitaire, Membre de l'Académie nationale de Médecine, Membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST)

EN SAVOIR PLUS

Renaissance Numérique et Syntec Numérique (mai 2019), *Tous acteurs des données. Appréhender les données pour mieux les valoriser*, 97 pp. : <https://www.renaissancenumerique.org/publications/tous-acteurs-des-donnees-apprehender-les-donnees-pour-mieux-les-valoriser>

Renaissance Numérique (mars 2017), *17 Experts / 36 propositions pour une ambition politique en matière de e-santé*, 44 pp. : <https://www.renaissancenumerique.org/publications/17-experts-36-propositions-pour-une-ambition-politique-en-matiere-de-e-sante>

Renaissance Numérique (septembre 2014), *D'un modèle de santé curatif à un modèle préventif grâce aux outils numériques*, 119 pp. : <https://www.renaissancenumerique.org/publications/d-un-systeme-de-sante-curatif-a-un-modele-preventif-grace-aux-outils-numeriques>



DIRECTION DE LA PUBLICATION

Bernard Astruc, Fondateur et Directeur des affaires médicales, Eutelmed

Jennyfer Chrétien, Déléguée générale, Renaissance Numérique

Pierre-Frédéric Degon, Responsable des affaires gouvernementales, Abbott France

RÉDACTION

Jessica Galissaire, Responsable des études, Renaissance Numérique

LE GROUPE DE TRAVAIL

Bernard Astruc, Fondateur et Directeur des affaires médicales, Eutelmed

Stéphanie du Boucher, Responsable des affaires publiques de Roche & Secrétaire générale, Fondation Roche

Arnaud Dechoux, Responsable des affaires publiques, Kaspersky France

Pierre-Frédéric Degon, Responsable des affaires gouvernementales, Abbott France

Jean-Marie Dunand, Directeur activité santé, Docaposte

Hector Duport de Rivoire, Responsable des affaires institutionnelles, Microsoft France

Valérie Marchand, Responsable de la filière santé, GS1 France

Anne-Sophie Mouren, Avocate associée au pôle Technologies, Médias et Télécommunications, Pinsent Masons

Roxana Ologeanu-Taddei, Professeure associée en management des systèmes d'information, Toulouse Business School

Annabelle Richard, Avocate associée au pôle Technologies, Médias et Télécommunications, Pinsent Masons

RELECTURE

Henri Isaac, Président, Renaissance Numérique

Nous tenons également à remercier **Mehdi Rafenne**, chargé de mission stagiaire au sein de Renaissance Numérique, qui a accompagné le groupe de travail tout au long de ses auditions.



À PROPOS DE RENAISSANCE NUMÉRIQUE

Renaissance Numérique est le principal think tank français indépendant dédié aux enjeux de transformation numérique de la société. Réunissant des universitaires, des associations, des grandes entreprises, des start-ups et des écoles, il vise à élaborer des propositions opérationnelles pour accompagner les acteurs publics, les citoyens et les acteurs économiques dans la construction d'une société numérique inclusive.

Renaissance Numérique
32 rue Alexandre Dumas - 75011 Paris
www.renaissancenumerique.org