COMMISSION BIOETHIQUE

Nos données de santé, à qui appartiennent-elles ?

Support à la réflexion conduite par la commission bioéthique

Enjeux sur vos données de santé

Le numérique, associé à la constitution de banques des données de santé personnelles, représente un progrès incontestable dans le domaine de la santé ; soutenir son développement est source d'avancées majeures.

Les freins à cette démarche forment un véritable obstacle pour la recherche médicale et induisent une attitude contraire à une éthique du progrès.

Le Règlement Européen sur la Protection des données de santé définit notamment les principes de l'information et du consentement de la personne et des conditions d'utilisation de ses données.
L'accès aux banques de données personnelles est encadré par des dispositions de protection de l'anonymat.
En France, la CNIL est chargée de contrôler l'application des règles relatives à la protection des données personnelles.
Il est recommandé aux personnes d'être vigilantes sur les données personnelles mises sur les réseaux sociaux. Le risque de récupération de ces données est susceptible de fragiliser l'anonymat des banques de données.

Une voie de passage éthiquement acceptable est à trouver entre protection des données et nécessité de partage. Ce partage est un élément central pour que notre système de santé progresse en qualité, en prévention et en efficacité.
L'utilisation accrue du numérique requiert un suivi attentif des banques de données non seulement pour en assurer leur cyber-sécurité mais également pour veiller à la protection des personnes.

Le progrès des technologies de l'information permet aujourd'hui la collecte et le traitement massif de données, de données personnelles et de données de santé.

Dans ce contexte, la commission bioéthique de l'APFDH a souhaité faire le point sur les droits détenus sur les données de santé et leurs titulaires en plaçant le patient au cœur de la réflexion éthique que soulèvent les données massives.

Le pouvoir, la maîtrise par le patient de ses données constituent-ils la clef d'un système vertueux et bénéficiaire pour tous les acteurs de santé ?

Les débats sur la "propriété" et l'exploitation des données personnelles de santé revêtent une acuité particulière face à la pandémie actuelle.

La question d'une utilisation des données de santé respectueuse des grands principes éthiques dont la F∴M∴est porteuse, se pose dans l'urgence. (Cf. avis du Comité consultatif National d'éthique, CCNE du 8 avril 2020).

1 - A qui appartiennent les données ?

1.1 - L'identification des droits sur les données et de leurs titulaires passe par leur qualification juridique.

Qu'est-ce qu'une donnée pour le droit ?

Le droit connaît les choses et les personnes.

Les choses peuvent être tangibles ou immatérielles, elles sont l'objet d'appropriation.

Les personnes sont titulaires de droits, notamment sur les choses.

La donnée semble à priori être une chose, un peu particulière car elle est immatérielle.

Sauf cas particulier défini par la loi, les données ne peuvent faire l'objet d'appropriation, elles sont de « libre parcours ». Néanmoins, l'absence d'appropriation n'exclut pas toute protection par le droit.

Qu'est-ce qu'une donnée de santé ?

La définition est donnée par l'article 4 du RGPD (Règlement Européen sur la Protection des données du 27 avril 2016 qui définit le droit commun du traitement des données à caractère personnel) :

« On entend par données concernant la santé les données à caractère personnel relatives à la santé physique et mentale d'une personne physique, y compris les prestations de service de soins de santé qui révèlent des informations sur l'état de santé de cette personne. »

L'article 4 poursuit :

« On entend par données à caractère personnel, toute information se rapportant à une personne physique identifiée ou identifiable » c'est-à-dire : « *une personne physique qui peut être identifiée directement ou indirectement, notamment par un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou par un ou plusieurs éléments spécifiques propre à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

La Loi Informatique et Libertés (LIL) du 6 janvier 1978 modifiée le 20 juin 2018 – section 3, articles 64-73, ainsi que l'ordonnance du 12 décembre 2018 reprennent ces définitions en les adaptant au droit français.

Les données à caractère personnel

Elles diffèrent des autres données par leur lien étroit avec l'individu.

Ce lien est d'autant plus étroit que les données concernent la santé.

Une donnée personnelle qui ne serait pas une donnée de santé par nature, le deviendrait du fait de son croisement avec d'autres données ou du fait de sa finalité, c'est-à-dire de l'utilisation qui en est faite au plan médical.

Cette relation à la personne est source pour les juristes d'une controverse : les données personnelles sont à la fois des prolongements de la personnalité de l'individu et des informations qui peuvent circuler, être reproduites. Elles sont à la frontière entre la personne et la chose.

Certains en déduisent un droit de propriété sur ces données, d'autres considèrent ces données comme l'expression de l'individualité de ces personnes, au même titre que son image, son corps ou l'expression de sa personnalité dans la création.

1.2 - Encadrement des données personnelles dans le droit positif.

Le RGPD ne reconnait pas un droit de propriété sur les données à caractère personnel.

Les données sont considérées comme des attributs de la personnalité des personnes concernées. Elles ne sont donc pas cessibles.

La protection des données à caractère personnel relève des droits fondamentaux de la personne.

Ces données sont dites sensibles et leur traitement, par principe, est interdit, sauf exception, notamment en cas de finalité d'intérêt public (article 9 du RGPD).

Toujours selon le RGPD, un traitement de données peut intervenir sur la base d'un consentement express de la personne concernée avec des limites tenant aux finalités du traitement des données, à l'absence de contre parties financières. Un droit de retrait du consentement est possible à tout moment (article 7-3 du RGPD).

Dans la droite ligne du RGPD, **le droit positif français** est irrigué par l'idée que « la personne dispose d'un droit de décider et de contrôler les utilisations faites des données à caractère personnel la concernant, logique dite d'autodétermination informationnelle ou de self data » (par opposition à un droit de propriété).

L'article 1 de la (la loi Informatique et Liberté, LIL) consacre expressément la logique du droit de la personne sur ses données et en fixe les conditions (article 1 modifié par article 54 de la loi 2016.1321 « Pour une République Numérique » du 7 octobre 2016).

1.3 - Quels droits pour le patient sur ses données de santé ?

Le principe de l'autodétermination informationnelle, inscrit dans le droit positif français, affirme les droits du patient tout en y apportant de nombreuses restrictions.

L'affirmation du droit des patients : Principes

Les patients doivent être informés des traitements de leurs données de santé :

- Les patients reçoivent une information et le cas échéant peuvent exercer leur droit à opposition pour les utilisations "usuelles".
- Les patients donnent leur consentement et disposent d'un droit de retrait de celui-ci pour les utilisations moins "usuelles".

Les patients peuvent exercer des droits sur leurs données de santé.

- Droit d'accès aux données, de rectification des données, de limitation des traitements, d'opposition aux traitements, d'effacement des données, de droit à la portabilité des données (articles 15 à 21 RGPD).
- Droit de donner des directives sur le sort des données après le décès (LIL art. 85 modifié par l'ordonnance du 12 décembre 2018 – transposition en droit français du RGPD).

En revanche les données de santé ne peuvent en aucun cas être vendues, que ce soit par le patient lui-même, ou par un tiers, avec ou sans l'accord du patient.

L'article 1111-8 chap. VII du code de la santé publique prohibe, sous peine de sanction pénale, "*tout acte de cession à titre onéreux de données de santé identifiantes, directement ou indirectement, y compris avec l'accord de la personne concernée*".

Des restrictions nombreuses sont apportées aux droits du patient sur ses données de santé, et notamment :

Si le patient bénéficie du droit de s'opposer au traitement de ses données, il doit justifier les motifs qui doivent être légitimes. Le texte cite « des raisons tenant à la situation particulière de la personne concernée ».

Le droit à l'effacement des données traitées (droit à l'oubli) n'est pas applicable en matière de traitement auxquels il est procédé dans le cadre de soins ou à des fins de recherche scientifique.

La poursuite d'un intérêt public important prévaut sur le droit pour un patient de ne pas subir de décisions thérapeutiques fondées exclusivement sur un traitement automatisé de données personnelles concernant la santé.

Le traitement est autorisé sans le consentement du patient, s'il est rendu nécessaire aux fins médicales de médecine préventive, de diagnostics médicaux, d'administration de soins ou de traitements dans l'intérêt public, pour éviter notamment la propagation de maladies.

Compte tenu de ces restrictions, le patient bénéficie-t-il alors du droit de décider du traitement des données de santé recueillies dans le cadre des soins ?

La loi prévoit au bénéfice du patient un droit clair d'accès aux données de santé le concernant, collectées dans le cadre des soins, avec la possibilité d'en obtenir copie.

C'est ce droit essentiel d'accéder aux données et de les détenir qui peut permettre la participation pleine et entière du patient aux soins qu'il reçoit et plus généralement au système de santé.

1.4 - Les droits des professionnels sur les données de santé

Des principes ou valeurs clés fondent la déontologie médicale :

Respect de la personne, Justice, Pertinence et Bienfaisance

Ces valeurs induisent le respect du secret médical, de la confidentialité des données dans le cadre du colloque singulier médecin-patient.

Les professionnels de santé ne peuvent pas vendre les données à caractère personnel des patients mais ils peuvent dans certains cas les échanger ou les partager (art. 1110-4 Code santé Publique, CSP).

L'échange de documents comportant des données de santé consiste en un flux de données visant à communiquer des données de santé à des destinataires clairement identifiés (ex : messagerie sécurisée).

Le partage vise à mettre à disposition de plusieurs professionnels fondés à les connaître, des données de santé utiles à la coordination et à la continuité des soins, dans l'intérêt de la personne prise en charge (ex : Dossier Médical Partagé, DMP).

Les professionnels concernés sont définis largement dans l'article R 1110-2 du CSP. Il s'agit des professionnels de santé (4e partie du CSP) et des professionnels du médicosocial et du social.

1.5 - Qu'en est-il des données anonymisées ?

Le droit des personnes concernées ne porte que sur les données à caractère personnel à l'exception des données anonymisées.

Le procédé d'anonymisation est défini comme "le résultat du traitement de données personnelles afin d'empêcher, de façon irréversible, toute identification". Il suppose, ni individualisation, ni corrélation, ni interférence : avis du G29 du 10 avril 2014, (le G29 regroupe toutes les structures et autorités homologues de la CNIL dans les Etats membres de l'Union Européenne)

Le RGPD n'est pas applicable aux traitements des données anonymisées : ainsi les droits accordés aux personnes concernées sur leurs données au titre du RGPD ne s'appliquent plus une fois les données anonymisées.

Le procédé d'anonymisation permet l'utilisation sans frein des données dans le cadre notamment de recherches scientifiques ou d'outils d'intelligence artificielle.

Se pose néanmoins la question de l'irréversibilité de l'anonymisation notamment avec le développement du numérique et le traitement des données massives. Ces questions renvoient à de nombreux enjeux éthiques liés au recueil et au traitement des données personnelles.

2 - Questionnements éthiques à l'ère des données massives.

2.1 - Les droits fondamentaux de la personne humaine sur ses données sensibles

Dossier patient et consentement

La relation de soin repose sur un rapport humain fondé sur la confiance, l'écoute, l'observation.

Pendant longtemps, la collecte des données concernant chaque personne malade a été effectuée sans son consentement explicite. Ces données constituaient « l'observation », fondement du dossier médical, propriété de l'institution.

Le dossier médical est devenu la propriété du patient à partir de la loi Kouchner du 4 mars 2002 relative au droit des malades et à la qualité du système de santé.

Son usage à des fins collectives (recherche médicale, aide à la décision) est donc devenu dépendant du consentement explicite et éclairé du titulaire du dossier.

Toutefois, les données n'appartiennent pas au patient au sens du droit de propriété. Par contre, le patient a des droits dessus, liés aux droits fondamentaux attachés à la personne humaine. Il est donc nécessaire de protéger ces droits, notamment en cas d'utilisation dans le cadre de la recherche.

La protection des droits du patient : notion de consentement libre et éclairé.

Les données recueillies dans le cadre d'une relation de soins ou via les données médico administratives sont ainsi considérées comme sensibles et bénéficient d'une protection.

Leur traitement est interdit (art. 8 de la LIL). Mais des exceptions existent pour la recherche et la santé si la personne a donné son consentement libre et éclairé.

La notion de consentement est cohérente avec la vision d'un droit à l'autodétermination informationnelle. Toutefois, le consentement n'atteint son plein effet que s'il est libre et éclairé, c'est-à-dire non présumé, expresse, préalable et assorti de la possibilité de le retirer.

De même il suppose une information claire et explicite des traitements éventuels sur ces données.

Cela suppose que le titulaire des données ait connaissance de ceux (acteurs de santé) qui pourront utiliser les données, de l'usage qu'ils entendent en faire dans l'immédiat et des usages potentiels qu'ils pourraient en faire dans l'avenir.

2.2 - Le numérique et l'apparition de données massives.

La numérisation des informations cliniques, paracliniques collectées dans les établissements de soins a permis la constitution de très grandes collections de données initiales. Il en résulte des évolutions et des questionnements sur les notions de données de santé et de consentement.

Evolution de la notion de données de santé

Les données massives (big data) sont définies ainsi dans l'avis 130 du CCNE « *Disponibilité d'un nombre important de données ou de données de taille importante, que seuls les outils du numérique allant de l'algorithme à la puissance de calcul des ordinateurs permettent de traiter efficacement* ».

Ces données massives offrent des opportunités majeures d'amélioration de prévention, de la qualité et de la sécurité des soins.

Elles posent cependant des questions éthiques qui portent notamment sur les modalités de l'information et du consentement des personnes concernées ou de l'expression de leur droit d'opposition, en fonction notamment des finalités de l'utilisation des données générées.

Les données massives se caractérisent par :

- un changement d'échelle,
- une pérennité,
- une diffusion dans le temps et dans l'espace,
- la génération de données secondaires,

ce qui constitue une rupture par rapport aux données recueillies classiquement et par rapport aux principes et valeurs éthiques, notamment ceux relatifs à la séparation vie publique-vie privée.

Une donnée en apparence anodine peut, une fois corrélée avec d'autres, donner une information sur la santé, d'où l'impossibilité de garantir sur le long terme l'efficacité d'une anonymisation de données sensibles. Il en résulte un risque de perte de confidentialité de la vie privée. Cette divulgation d'informations privées peut être le fait de la personne elle-même sur les réseaux sociaux.

L'élargissement de la notion de donnée de santé.

Toute information primaire, issue du dossier patient ou de toute autre source (personnelle, administrative, …) peut contribuer à une information sur la santé en raison de la possibilité de la réutiliser, de la croiser avec d'autres données qui ne lui sont pas liées.

Ce traitement fait apparaître de nouvelles informations déduites (données secondaires) qui peuvent être des données personnelles, sensibles, et identifiantes.

Sauvegardées, ces données secondaires peuvent être utilisées à l'insu des titulaires des données initiales.

Il serait donc impossible de définir à priori une donnée de santé. Comment alors caractériser une donnée comme sensible ?

La notion de données de santé ne peut plus se limiter aux données personnelles recueillies dans le cadre du soin, c'est-à-dire aux données par nature recueillies dans le cadre d'une prise en charge médicale.

La notion de données de santé inclut celles obtenues par croisement avec d'autres données (par exemple issues d'une application sur smartphone, …) et celles obtenues par destination (ex : informations utilisées par une société d'assurances à partir de selfies, …) et qui peuvent être utilisées dans le parcours de soins.

C'est au bout du compte la finalité du traitement, c'est-à-dire l'utilisation qui en est faite au plan médical, qui qualifie de données de santé des données qui ne le sont pas à priori.

COMMISSION BIOETHIQUE

Par qui et pourquoi des données de santé peuvent-elles être utilisées ?

La question se pose avec l'apparition de nouveaux acteurs.

Le risque vient de l'intervention, dans le soin et le marché de la santé, de nouveaux acteurs : les experts de la gestion et de l'analyse des données qui conçoivent des modèles et des algorithmes.

Les initiatives peuvent venir du patient lui-même qui partage avec d'autres patients des informations médicales. Elles peuvent venir aussi d'entreprises privées qui, avec les objets connectés, les réseaux sociaux incitent les individus à devenir acteurs de leur propre santé.

Ces entreprises privées n'ont pas pour finalité le soin.

Le principe demeure que les données sensibles ne peuvent être utilisées que par le patient lui-même et à des fins de traitements médicaux.

Ce principe comporte des exceptions qui nécessitent le consentement du titulaire des données.

La notion de consentement est-elle impactée par le traitement de données massives ?

Comment, dès lors, le consentement du patient à l'utilisation de données sensibles le concernant va-t-il pouvoir s'exercer ?

<u>Evolution de la notion de consentement dans le cas de traitement de données massives.</u>

La question de l'information et du consentement individuel.

Dans la relation médecin-malade, ce dernier est informé de la démarche utilisée par le médecin. Ceci implique qu'il soit informé d'un recours au traitement de données massives (ex : pour interpréter des images,…).

Mais le patient n'est pas tenu de donner son consentement spécifique à l'utilisation de données personnelles collectées dans le cadre de cette prise en charge, le médecin étant soumis au secret médical et donc à la confidentialité des données.

En revanche, la question se pose lors de l'utilisation ultérieure de ces données pour la constitution d'une collection ou d'un entrepôt pour une recherche clinique.

Si son consentement n'est pas requis, le patient doit cependant être informé. Il peut s'opposer à cette utilisation, demander communication des données, et aussi utiliser son « droit de ne pas savoir. »

L'avis 130 du CCNE précise : « *Les nouvelles technologies questionnent sur le plan éthique : l'information délivrée à la personne et son consentement au recueil et à l'utilisation des données personnelles sont devenus plus complexes, dès lors que les données sont aisément dupliquées et réutilisées à des fins non initialement définies et que leur traitement fait apparaître de nouvelles données dites secondaires, souvent plus sensibles que les données initiales et identifiantes.* »

Ceci questionne la notion même de consentement.

« *Ce dernier n'atteint son plein effet que s'il est libre et éclairé.* »

Or les données massives prennent souvent une dimension trop grande pour être appréhendées par l'individu.

Le titulaire des données est dans une situation d'infériorité par rapport à un opérateur, notamment les GAFA, qui lui offre par ailleurs une prestation de service.

De nombreuses questions se posent alors :

Y a-t-il une alternative à la question du consentement individuel ?

Comment assurer maîtrise et contrôle ? Quelle régulation ?

Et ce d'autant plus que le traitement de multiples données (santé, mode de vie, environnement de la personne, …) permet une approche individualisée de la prédiction d'une maladie, de sa prévention, de la thérapeutique. Le traitement des données massives constitue ainsi une avancée majeure qui ouvre la voie à une médecine personnalisée. Comment garantir ce gain sur la qualité et la sécurité des soins ?

Le questionnement éthique se situe dans ce paradoxe entre protection de l'individu et

amélioration de la qualité et de la sécurité des soins. Où se situe le point d'équilibre ?

Le droit européen réaffirme le principe de spécialité du consentement.

Le RGPD, la Loi Informatique et Liberté (LIL) le Code de la Santé Publique (CSP) confirme le principe d'interdiction de traitement des données de santé. Mais de nombreuses exceptions sont prévues, notamment lorsque la finalité du traitement l'exige.

Il s'agit des cas suivants :

- Traitements des données pour lesquels la personne a donné son consentement express.
- Traitements des données comportant des données concernant la santé, justifiés par l'intérêt public.
- Traitements des données portant sur des données à caractère personnel rendues publiques par la personne concernée.
- Traitements des données nécessaires à la recherche publique.

➢ Si le consentement n'est pas requis, l'information doit être délivrée d'une façon concise, transparente et aisément accessible. Ces informations sont fournies par écrit (RGPD confirmé par LIL).

L'article 5 du RGPD érige en principe la valeur de transparence.

On assiste à un passage progressif d'une volonté de contrôle a priori à une logique d'intervention et de contrôle a posteriori, fondée sur une recherche d'intelligibilité, de responsabilisation des acteurs et de loyauté vérifiable des responsables du traitement des données.

Cette démarche se fonde sur une relation de confiance entre le titulaire des données et ceux qui les recueillent, les traitent et y ont accès.

Mais la complexité des processus ne permet pas à un particulier de se livrer lui-même à un contrôle.

Selon le CCNE (avis 130, préalable à la révision de la loi bioéthique), le particulier ne devrait accorder sa confiance et ne consentir à l'utilisation de ses données personnelles que si celle-ci se fait dans le cadre d'une gouvernance identifiée par un responsable désigné, ayant pris des engagements clairs, engagements vérifiables par une autorité de contrôle. Il convient aussi que le public soit largement informé.

➢ Lorsque le consentement est requis, se pose la question de son recueil, garantissant le respect des droits fondamentaux et de l'information du patient.

Dans ce cas le consentement ne peut être unique et homogène. Il doit être adapté à chaque situation particulière et garantir la confiance.

En tout état de cause, le risque est celui d'une "délégation de consentement" à des décisions fournies par algorithmes et le danger d'une "minoration" de la prise en compte des situations individuelles, lorsque celles-ci ne relèvent pas expressément de l'objet de l'algorithme utilisé.

<u>De nouvelles formes de consentement pour faciliter l'accès aux données ?</u>

Un droit collectif sur les données de santé ?

N'y a-t-il pas conflit d'intérêt, ou au moins des enjeux différents face à un double impératif.

Pour la recherche, l'impératif est d'un accès large aux données et de leur partage dans l'intérêt général.

Pour l'individu, c'est celui de la protection de ses droits individuels.

Quelle place alors pour le consentement de la personne ?

De nouvelles formes de consentement et d'accès aux données se manifestent.

L'idée d'un droit collectif sur les données de santé émerge, qualifié de droit à la science.

Le modèle traditionnel du consentement ne semble plus approprié pour un grand flux de données ni pour un partage généralisé.

D'autres modes de consentement sont discutés :

- Consentement large qui ne donne pas une finalité précise mais un champ d'application.
- Consentement à options.
- Consentement dynamique, le titulaire est considéré comme participant à la recherche.

- Consentement présumé, les données peuvent être utilisées sauf en cas de refus explicite par la personne (sur le modèle des prélèvements d'organes).

Si les données sont complètement anonymisées, elles ne peuvent être qualifiées de personnelles et ne relèvent pas du RGPD ni de la LIL.

L'accès à ces données est alors libre.

Cependant l'anonymisation pose question.

Si elle est irréversible, elle ampute les données d'une bonne part de leur utilité.

Pour éviter la perte de données, on applique une **pseudonymisation** : un numéro remplace une identité mais on peut en retrouver la trace. La réidentification ultérieure ne peut plus être exclue.

Peut-on alors éthiquement se dispenser du consentement, même dans ce cas ?

Une réflexion s'impose sur la notion de consentement au traitement des données massives et qui devrait porter sur l'objet du consentement d'une part, les modalités de son recueil d'autre part, afin d'assurer un équilibre entre le respect du droit des personnes et la dynamique des usages.

La notion de bien commun peut aider à cette réflexion s'agissant de l'intérêt de la recherche, de l'enrichissement des connaissances au bénéfice de tous.

C'est in fine sur une relation de confiance et de réciprocité que reposera le consentement et non pas sur une définition restrictive des finalités, établie a priori.

Le débat se situe entre consentement individuel et confiance collective (Cf. avis 130 du CCNE).

Le consentement est une des bases juridiques du traitement des données personnelles.

Lorsqu'il est requis, il peut prendre différentes formes, essentiellement pour faciliter la recherche à condition que l'information de la personne et la protection de ses droits individuels soient assurées. C'est là une conception individualiste de la relation de la personne à ses données.

D'autres conceptions émergent.

Les données personnelles relatives à la santé deviennent aussi, par leur mise en commun, les composantes d'un réseau d'informations utiles à l'intérêt général.

Ce réseau constituerait un bien commun, relevant d'une protection collective de la vie privée.

Va-t-on vers un droit collectif sur les données de santé ? Deux approches s'opposent :

Approche libérale : maximisation des libertés individuelles par le biais du consentement et de la patrimonialisation des données.

Approche communautaire et collective qui pourrait exiger une limitation de certaines libertés individuelles au nom de l'intérêt général et du bien commun.

La recherche d'un point d'équilibre entre l'individuel et le collectif est au cœur du débat éthique, entre l'autonomie de chacun et la protection que requiert l'utilisation généralisée des technologies recourant au traitement de données massives, protection qui ne peut reposer que sur une approche collective pour être efficace.

2.3 - La notion de "garantie humaine" sur la qualité des données.

Une chose est le consentement au traitement des données.

Autre chose, tout aussi fondamental quant aux enjeux éthiques du traitement des données massives, est la garantie de la qualité des données issues de ce traitement, la qualité des conclusions tirées par le système, de leur

exploitation, ainsi que la fiabilité des décisions induites du traitement des données.

Les risques sont ceux de décisions erronées, de discrimination.

La notion de garantie humaine abordée dans le rapport Gruson (novembre 2018) a pour objet de répondre de la rigueur méthodologique, c'est-à-dire :

- de la qualité des données.
- de l'adéquation des traitements algorithmiques à la question posée.
- de la vérification, sur un jeu de données indépendantes, de la robustesse et de l'exactitude du résultat donné par l'algorithme.

Cette garantie humaine doit s'exercer de façon répétée.

Elle impose que les professionnels de santé, chercheurs, experts, soient formés et que les sites et applications, hors parcours de soins, soient évalués sur le plan qualitatif.

La notion de garantie humaine permet d'encadrer la responsabilité des professionnels et des opérateurs.

Cette notion est reprise dans le projet de loi bioéthique.

L'article 11 du projet de loi Bioéthique vise à sécuriser la bonne information du patient lorsqu'un traitement algorithmique de données massives est utilisé à l'occasion d'un acte de soins.

Il décline également la garantie d'une intervention humaine qui serait érigée en principe législatif et qui encadrerait la responsabilité du professionnel recourant à l'Intelligence Artificielle.

Dans le cadre de cette responsabilité, il incombera au professionnel de santé un devoir d'information du patient et l'obtention de son consentement éclairé.

Il s'agit néanmoins d'une garantie formelle qui n'exclut pas des dérives. D'où la nécessité d'une supervision, d'un pilotage à l'échelle des établissements de santé mais aussi à l'échelle nationale.

La garantie humaine du numérique en santé pourrait être assurée par des procédés de vérification régulière « ciblée et aléatoire » des options de prise en charge proposées par les dispositifs numériques et par un deuxième "regard médical humain" à la demande du patient ou du professionnel de santé.

En tout état de cause, l'objectif demeure toujours celui du meilleur soin pour tous, sans discrimination aucune, et dans le respect des droits fondamentaux de la personne humaine sur ses données sensibles.

2.4 - Pour un régime de consentement à l'utilisation des données de santé considérées comme un élément du corps humain ?

La compréhension de ce que nous révèlent les données de santé, nécessite de passer de l'échelle individuelle à l'échelle collective.

Le régime de consentement à l'utilisation des données de santé regardées comme éléments du corps humain reste le consentement libre et éclairé, explicite de son vivant. Toute opposition formelle pourrait passer par l'inscription sur le Registre National Des Refus, RNR.

En effet, au titre de l'article 16 du code civil, "le corps est inviolable et ses éléments et ses produits ne peuvent faire l'objet d'un droit patrimonial" (article 16-1).

De plus l'article 16-3 précise qu'il ne peut être porté atteinte à l'intégrité du corps humain qu'en cas de nécessité médicale pour la personne ou à titre exceptionnel dans l'intérêt thérapeutique d'autrui. Le consentement de l'intéressé doit être recueilli préalablement hors le cas où son état rend nécessaire une intervention thérapeutique à laquelle il n'est pas à même de consentir.

Le registre national des refus prévoit l'expression de l'opposition selon trois hypothèses d'utilisation d'éléments du corps :

- pour une greffe d'organes et/ou de tissus (thérapeutique)
- pour la recherche scientifique (différent du don du corps à la science)
- pour rechercher la cause du décès : autopsie médicale (excepté les autopsies

judiciaires auxquelles nul ne peut se soustraire).

Depuis le 1er janvier 2017, l'expression du refus peut, outre l'inscription au RNR, se faire par un écrit circonstancié du défunt de son vivant, ou de deux témoins attestant par écrit de cette expression ou par la transcription par les proches du témoignage oral d'une telle opposition.

A l'image des exemples précédents, il pourrait être imaginé la possibilité d'opposition par une personne, à l'utilisation de ses données de santé à toute autre fin que mon intérêt thérapeutique ou l'intérêt thérapeutique d'autrui.

Selon cette proposition, il appartient au législateur de formuler en des termes adaptés qui permettraient de cette façon simple et déjà largement pratiquée pour le don d'organes et de tissus, (registre National des refus) l'élargissement de cette expression du refus d'utilisation aux données de santé, en ce qu'elles sont des produits du corps humain.

En Conclusion :

Le XXIème siècle est marqué par le développement des réseaux sociaux et par des avancées technologiques considérables telles que l'intelligence artificielle, les objets connectés, par exemple. Une multitude d'informations concernant notamment notre santé sont dorénavant stockées par des algorithmes (big data, géants du numérique) dont la puissance et l'intelligence sont exponentielles.

Or nul ne souhaite voir apparaître sur les réseaux sociaux son nom, son adresse, son dossier médical. Le piratage et la divulgation des données d'un laboratoire, qui se sont produits tout récemment, montrent à quel point la protection de la vie privée est primordiale. La sécurisation des données de santé doit se réaliser tant au plan technologique que juridique.

Par ailleurs, l'exploitation de ces données offre un potentiel extraordinaire pour la recherche et les progrès de la médecine. On assiste à des alliances entre laboratoires pharmaceutiques et Big techs par exemple ou entre sociétés technologiques qui conduisent à une véritable « plateformisation » de la santé. Afin de préserver la vie privée, l'accès aux banques de données personnelles, pour une utilisation d'intérêt général, est encadré par des dispositions relatives à la protection de l'anonymat.

L'enjeu éthique est de trouver un équilibre entre protection des données et nécessité de partage. Ce partage est un élément central pour que notre système de santé progresse en qualité, en prévention et en efficacité, sans remettre en cause les droits fondamentaux de la personne.

Le Règlement Général sur la Protection des données (RGPD) européen, complété par des lois nationales, encadre notamment l'information et le consentement de la personne sur les conditions d'utilisation de ses données. Cette règlementation est-elle suffisante face aux enjeux éthiques, sanitaires, économiques ?

■ ■ ■