IA et santé

Poullet, Yves

Published in:
Pour des Intelligences artificielles au service du corps vulnérable

Publication date:
2023

Document Version
le PDF de l'éditeur

IA et santé – A la lumière de quelques textes réglementaires

L'intelligence artificielle dans le secteur médical : les défis du droit face à la santé « intelligente » ?

Yves POULLET

Professeur associé à l'UCLille, Professeur émérite à l'UNamur,
co-Président du NADI (Namur Digital Institute)

Résumé : L'intelligence artificielle envahit les pratiques médicales et multiplie les outils au service de la santé. Ces technologies modifient profondément la relation entre professionnels de la santé et les patients, laisse entrevoir la perspective d'un homme augmenté y compris dans son bagage génétique et introduit de nouveaux acteurs dans le secteur des soins. L'article recense tant les bénéfices que les dangers liés à l'utilisation de ces technologies, risques liés tant à la nature opaque et non exempte d'erreurs et de biais de cette technologie, que de la déshumanisation de la relation entre un professionnel de plus en plus contraint à suivre la vérité sortie des ordinateurs et un patient réduit à ses seules données. La seconde partie de l'article analyse la réponse du droit à ces défis lancés par l'IA. Les applications de l'IA dans le domaine médical se voient encadrées en particulier par trois textes : le premier est certes le règlement relatif à la protection des données ; le deuxième souvent inaperçu par les juristes réfère au règlement de 2017 relatif aux dispositifs médicaux, y compris suivant l'interprétation hardie de la CJUE, les logiciels d'IA ; le troisième attend son approbation finale par les autorités européennes : il s'agit de la proposition de règlement sur l'IA, qui introduit en particulier vis à vis des applications dites "à haut risque" des obligations, notamment, de gestion et d'évaluation interdisciplinaire et "multistakeholders" à propos des impacts de l'application envisagée. En conclusion, les promesses de l'intelligence artificielle, en particulier dans le domaine de la santé, invitent à lui confier de plus en plus le soin de nos corps. Mais encore faut-il se rappeler qu'il ne s'agit là, au sens propre, que d'artifices de notre intelligence humaine et qu'à ce titre nous devons nous nous méfier des raccourcis que souvent notre cerveau emprunte et qui conduisent à tant de biais et d'erreur. Que ces technologies soient dignes de notre confiance (Trustworthy AI), exige notre prudence et notre maîtrise. C'est cette prudence et à cette maîtrise continues, qui constituent les mots-clés du droit européen naissant de l'intelligence artificielle.

Mots-clés : Intelligence artificielle (IA), RGPD, Règlement IA

1. Le fil rouge du propos – L'intelligence artificielle envahit tous les domaines, celui de la santé en particulier. Ses promesses font rêver. Que l'on y songe : nos algorithmes prédisent mieux que nos meilleurs praticiens nos maladies actuelles et futures ; aident, comme l'ont montré récemment les initiatives prises en matière de la COVID-19, à la fois à mieux comprendre le fonctionnement du virus, mais également à lutter effectivement contre sa propagation ; accroissent les capacités de nos cerveaux ; transforment notre bagage génétique ; participent à des opérations chirurgicales avec une précision jamais atteinte… bref, que de bénéfices attendus de ces technologies hier de science-fiction aujourd'hui réalité ! Tel est l'objet de notre premier chapitre.

Le deuxième chapitre relit les promesses de l'outil à l'aune de quelques réflexions éthiques : la « datification » de nos êtres et de nos comportements conduit à s'interroger à propos de la déshumanisation de nos relations avec le corps des soignants ; le caractère prédictif de l'intelligence artificielle soulève des dangers accrus vis-à-vis de nos libertés individuelles et de discrimination entre individus ; les technologies conduisent à augmenter les capacités humaines, demain à modifier nos identités au mépris, on peut le craindre, de notre dignité humaine et au risque d'une société duale fondée sur la capacité réservée à certains d'accéder à de telles technologies. Enfin, la technologie fait entrer dans le secteur des soins de nouveaux acteurs : les « Medtechs » et il faut bien reconnaître que de plus en plus les développements d'intelligence artificielle sont aux mains d'entreprises seules capables par leur détention de *big data* de développer des systèmes d'intelligence artificielle dans différents domaines.

Le troisième nous invite à étudier la réponse du droit, actuelle ou en construction. Nous partirons pour ce faire des trois qualifications majeures assignées par le droit aux opérations couvertes par le présent propos. Il est indéniable que ces opérations constituent des traitements de données le plus souvent à caractère personnel et cette qualification nous amènera à analyser l'application des dispositions du RGPD à ces systèmes d'intelligence artificielle. A cette première qualification, on ajoute celle de « dispositif médical » dans la mesure où la jurisprudence européenne n'a pas hésité à élargir cette notion aux logiciels utilisés à l'appui d'interventions ou de décisions médicales. Le Règlement européen de 2017 encadre le développement et l'utilisation de tels dispositifs. Enfin, la proposition de la Commission, actuellement en discussion, relative aux technologies de l'intelligence artificielle mérite notre attention. Elle introduit une réglementation fondée sur une approche préventive et fondée sur le niveau de risques liés à une application. Trois angles d'attaque et des réglementations non nécessairement cohérentes et complémentaires nous obligeront à imaginer des voies de solution.

Il sera alors temps de conclure.

1 D'une définition aux multiples dimensions de la médecine du futur

2. A la recherche d'une définition – La notion d'intelligence artificielle est l'objet de nombre d'analyses et de discussions. Nous nous en tiendrons pour les besoins de notre propos à la définition courante reprise par Wikipédia : « L'intelligence artificielle (IA) est « *l'ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence* » ou celle plus parlante du créateur

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

du concept, J. MINSKY[1] : « *the building of computer programs which perform tasks which are, for the moment, performed in a more satisfactory way by humans because they require high level mental processes such as : perception learning, memory organization and critical reasoning* ». A ce foisonnement de définitions dans les ouvrages scientifiques, s'opposent la prudence des textes réglementaires qui hésitent à définir le concept. L'article 3 de la récente proposition de règlement de la Commission européenne du 21 avril 2021, dite AI Act[2], s'y risque cependant : « *système d'intelligence artificielle » (système d'IA), un logiciel qui est développé au moyen d'une ou plusieurs des techniques et approches énumérées à l'annexe I et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit* ». L'annexe[3] distingue ainsi différentes techniques ou approches dites d'intelligence artificielle, en particulier celles dites d'IA forte fondées sur l'apprentissage machine (*machine learning),* celles dites d'IA symbolique ou faible (les systèmes experts) et celles classiques fondées sur les statistiques.

Ainsi, on distingue, d'une part, ce qu'il est convenu d'appeler l'IA « symbolique », qui s'entend de l'exécution d'un programme traduisant le raisonnement tenu par des experts humains[4] et, d'autre part, l'IA « agrégationnel » : la machine ou plutôt des logiciels au fonctionnement complexe mettant en jeu différents réseaux de neurones traitant des multitudes de données présentes dans de vastes bases de données. Face à des données nouvelles, elles croisent celles-ci et sont capables dès lors de générer le résultat attendu par le programme, qu'il s'agisse d'une décision, d'une recommandation, d'une prévision. On ajoute que le système se nourrit de sa propre production et peut dès lors évoluer dans son fonctionnement. En d'autres termes, dans le cas de systèmes experts, le fonctionnement du système suit l'algorithme défini par le concepteur du système, ce dernier ayant, dès lors, la totale maîtrise du traitement. Dans les systèmes IA dits forts, les algorithmes de départ, une fois confrontés aux données auxquelles le système est appliqué, s'enrichissent par les croisements aléatoires opérés entre les données et découvrent ainsi de nouvelles règles. Bref, le système d'IA est auto-apprenant et évolutif au hasard des données rencontrées. Les algorithmes de fonc-

[1] Minsky né en 1927 (doctorat en 1954) est cofondateur, avec l'informaticien John McCarthy du Groupe *d'intelligence* artificielle du Massachusetts Institute of Technology (MIT).

[2] Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, SEC(2021) 167 final – SWD(2021) 84 final – SWD(2021) 85 final, 21 avril 2021, COM(2021) 206 final, disponible en ligne sur https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN (consulté le 26 mai 2021), en abrégé "Artificial intelligence Act". A noter que cette même proposition prend soin d'ajouter que le système peut être embarqué dans un dispositif matériel comme c'est le cas des robots intelligents : « *Le terme « intelligence artificielle » (IA) désigne un système qui est soit fondé sur des logiciels, soit intégré dans des dispositifs matériels, et qui fait preuve d'un comportement intelligent, notamment en collectant et traitant des données, en analysant et en interprétant son environnement et en prenant des mesures, avec un certain degré d'autonomie, pour atteindre des objectifs spécifiques.* » (art. 1 f.).

[3] *« Approches d'apprentissage automatique, y compris d'apprentissage supervisé, non supervisé et par renforcement, utilisant une grande variété de méthodes, y compris l'apprentissage profond ; Approches fondées sur la logique et les connaissances, y compris la représentation des connaissances, la programmation inductive (logique), les bases de connaissances, les moteurs d'inférence et de déduction, le raisonnement (symbolique) et les systèmes experts. ; Approches statistiques, estimation bayésienne, méthodes de recherche et d'optimisation. »*

[4] Par exemple dans le domaine de l'application du droit, la mise au point d'un logiciel qui structure l'ensemble des dispositions civiles et fiscales en matière de régime successoral et permet à ses utilisateurs de proposer la solution idéale pour la personne eu égard à sa situation patrimoniale et familiale

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

tionnement du système d'IA lui permettent de s'écarter du mode de fonctionnement de départ, présent dans l'algorithme préalable de base et échappent partiellement ou substantiellement aux concepteurs de base. Ce dernier peut, en effet, soit encadrer le fonctionnement du système dans le cadre d'un 'modèle'[5] et/ou, dans le cadre de tests, « superviser » le fonctionnement de l'algorithme pour éviter des dérives ou des résultats inattendus ou non souhaités, soit, enfin, au contraire, abandonner à la machine son fonctionnement : c'est ce qu'il est convenu d'appeler le '*deep learning*'[6],

3. IA *everywhere* – Le domaine médical est sans doute l'un des plus prometteurs pour le développement d'applications d'intelligence artificielle. La pandémie de la COVID-19 illustre bien la variété des champs d'intervention de l'IA. Ainsi, l'IA permet de mieux comprendre l'épidémie dans ses causes (recherche médicale) et peut prédire de manière fine sa propagation. Elle devient un outil de prévention de la communication de la maladie par la mise sur pied de systèmes de surveillance des personnes et de lutte contre l'« infodémie ». Enfin, elle optimise les soins à délivrer contre la COVID aux personnes[7]. Si le succès de l'IA en médecine se justifie par l'importance des bénéfices obtenus et attendus des applications de l'IA dans un domaine vital pour chacun de nous, elle s'explique également par l'importance des données susceptibles désormais d'être collectées et dès lors la possibilité de constituer des mégadonnées ou *big data,* dont l'existence est une condition même du développement d'outils de *machine learning.* Comme le note le Conseil National de l'Ordre des Médecins (en abrégé CNOM) dans son Livre Blanc « *Médecins et patients dans le monde des Data, des algorithmes et de l'intelligence artificielle* »[8], « *la transformation numérique de la médecine et la vision de la médecine du futur recouvrent des concepts et des avancées scientifiques et techniques aussi diverses que le traitement, l'analyse et le stockage des données de santé (sous les termes grand public de « big data » et de « cloud »), les algorithmes, l'intelligence artificielle et l'apprentissage machine, la génomique (et autres données « omiques »), les objets connectés (Internet des objets), la robotique, la réalité virtuelle augmentée, l'impression 3D, etc. ».* Diverses phases du traitement des données sont ainsi affectées et servent au développement de l'intelligence artificielle, depuis la collecte, le stockage et bien évidemment l'exploitation par les systèmes d'intelligence artificielle de toutes ces données collectées et stockées.

---

[5] *« Le terme « modèle » est une abstraction mathématique utilisée dans les méthodes d'apprentissage automatique qui fournit une description simplifiée des données pour résoudre la tâche à effectuer. ». (art.1.e)*

[6] « *Par système d"apprentissage profond ou d'apprentissage en profondeurù34ù (en anglais : deep learning, deep structured learning, hierarchical learning) est un ensemble de méthodes d'apprentissage automatique tentant de modéliser avec un haut niveau d'abstraction des données grâce à des architectures articulées de différentes transformations non linéaires.* » (Commission d'enrichissement de la langue française, « Vocabulaire de l'intelligence artificielle (liste de termes, expressions et définitions adoptés) », *Journal officiel* de la République française n° 0285 du 9 décembre 2018)

[7] L'ouvrage de Y. MENECEUR (*L'intelligence artificielle en procès,* Bruylant, 2021, p. 131 à 135) relate la manière dont les recherches sur les causes, la nature et la diffusion de la COVID-19 ont été menées tant en Chine, aux Etats Unis, au Canada tant par les pouvoirs publics que privés (en particulier à propos de la nature du virus : Deep Mind de Google, Alibaba DAMO Academy, Blue Dot canadien …), Sur ces divers aspects et les applications développées en la matière, lire N. NEVEJANS, « Les aspects juridiques et éthiques de l'utilisation de l'IA comme outil de lutte contre la Covid-19. », *Actes du Colloque de Lille,* (sous la direction de D. DOAT et Y. POULLET) 4 février 2021, L'Harmattan, Paris, 2022, à paraître. Cf. également, *Solutions numériques contre la COVID-19,* Conseil de l'Europe, Rapport, Octobre 2020.

[8] *Livre blanc et recommandations*, Janvier 2018, disponible sur le site : https://www.conseil-national.medecin.fr/sites/default/files/cnomdata_algorithmes_ia_recommandations_0.pdf.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

4. La collecte des données – La première consiste en la mise à profit jusqu'ici non souhaitée, du moins dans la médecine traditionnelle, des données récoltées et l'exploitation des potentialités de collecte de nouvelles données qu'offrent les technologies du numérique, comme *l'Internet of Things*, la m-santé, voire les données spontanément émises par les patients dans les réseaux sociaux, les chatbots, les forums de discussion et l'interrogation de moteurs de recherche afin de les structurer, de les organiser et de les exploiter. Ainsi, parmi les sources susceptibles d'alimenter les systèmes d'IA en santé, la CNOM[9] cite : « *1. les données médico-administratives produites par l'Assurance maladie (Sniiram) et les hôpitaux (PMS) ; 2. les données figurant dans les dossiers médicaux, à l'hôpital et en ville ; 3. les données détenues par des acteurs publics ou privés recueillies auprès de patients (essais cliniques notamment) ou de professionnels de santé ; 4. les données générées par les objets connectés, les applications mobiles, les sites Web et moteurs de recherche ; 6. les données de contexte* ».

Parmi ces sources, on en épingle deux en particulier : la récolte auprès des patients identifiés ou non, voire de chacun d'entre nous *via* les réseaux spécialisés ou non, collecte consciente ou non, des données dans le cadre de l'utilisation des systèmes dits de '*quantified self*' (ou 'automesure connectée', selon le vocabulaire adopté par la Commission générale de terminologie et de néologie). Cette appellation désigne les outils (objets connectés : parquets ou bracelets intelligents, mais également des implants dans le corps humain), les principes et les méthodes permettant, *via* des applications mobiles ou le Web, à chacun de mesurer ses données personnelles, de les analyser et de les partager. Il s'agira de données tantôt de prises de température, d'analyse de la tension, du rythme cardiaque, du taux d'insuline, etc. Si ces systèmes procurent des bénéfices, ils soulèvent cependant des questions délicates de sécurité accrues par la sensibilité des données collectées et leur nécessaire protection[10]. Certains de ces systèmes permettent par ailleurs aux patients de prendre en charge leur maladie, voire à distance d'effectuer la surveillance régulière de l'état de santé de ceux-ci.

Par ailleurs, on soulignera la multiplication de certains implants corporels dont la fonctionnalité est non seulement de collecter les données du patient, mais également de pouvoir, le cas échéant, intervenir vis-à-vis d'eux[11]. Le but est ici d'améliorer le corps au niveau fonctionnel et technique, d'atteindre une fusion homme-machine, de tendre vers le Cyborg. Ainsi, des stimulateurs de mémoire et des régulateurs du stress sont déjà largement utilisés. On pointe également la mise au point d'un système électronique doté d'un stimulateur cérébral pour traiter automatiquement certains problèmes cérébraux, comme la maladie de Parkinson et les crises d'épilepsie. Ce stimulateur détecte préventivement les crises et envoie des signaux électriques dans certains endroits du cerveau afin de les empêcher. Des robots fonctionnent comme des organes artificiels : on cite notamment l'ARGUS II[12] qui utilise une caméra vidéo branchée sur des électrodes qui stimulent la rétine de manière à permettre de discerner

[9] Voir le rapport déjà cité note, p. 12. Voir également le débat organisé par la CNOM suite au Livre Blanc, Débats de l'ordre, 10 janvier 2018, disponible à l'adresse : https://www.conseil-national.medecin.fr/node/2482/dbf104df

[10] Celia Rosas, « *The Future is Femtech : Privacy and Data Security Issues Surrounding Femtech Applications* », *Hastings Business Law Journal*, vol. 15, n° 2, 1er Juillet 2019, p. 319.

[11] Ainsi, des systèmes basés sur des implants corporels.

[12] https:// Argus II – Retinal Implant – Bionic Eye – Retinal Prosthesis System – the innovation station (tis.tv).

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

des formes et des mouvements ou l'implant COCHLEAR qui permet artificiellement aux sourds de retrouver l'ouïe. On souligne que ces systèmes, s'ils apportent d'incontestables bénéfices à la personne concernée, ont pour effet de mettre cette dernière à la merci du système, de la sécurité de celui-ci et des hackers, mais aussi des décisions prises par les entreprises qui commercialisent ce type d'implants… et, le cas échéant, les données ainsi collectées *via* ces implants.

Des puces électroniques intelligentes permettront – la science en est aux premières expériences, notamment dans le contrôle des pilotes d'avion – de lire la pensée d'autrui, voire de l'influencer[13]. Ces avancées posent deux questions éthiques majeures : celle de la discrimination : qui aura accès à de telles technologies qui permettent d'envisager un homme augmenté ?, et celle de la dignité humaine face aux risques de manipulation d'autrui. Ainsi, le projet de NEURALINK de soigner l'autisme et la schizophrénie par des implants électroniques corporels est contesté par la National Autistic Society sur base du principe que ces « maladies » sont constitutives de l'identité des personnes concernées. Nous reviendrons sur ces risques dans le troisième chapitre non sans avoir souligné l'importance des investissements que certaines entreprises consentent pour le développement de ces techniques d'« intelligence augmentée ».

5. La 3D au service de la médecine – Un rapide mot à propos de l'utilisation dans le domaine médical de l'impression 3D. Selon Wikipédia, l'impression 3D ou 'fabrication additive' regroupe les procédés de fabrication de pièces en volume par ajout de matière en couches successives depuis une modélisation 3D. C'est en effet grâce à cette technologie, qu'a été permise la création à un coût raisonnable d'exosquelettes personnalisés (hanches, bras[14] mais également appareils dentaires ou auditifs)[15]. On ajoutera la création en *open source* d'un robot humanoïde (*In Moov*[16]) avec des bras articulés directement par des impulsions du cerveau. Sans doute, faut-il craindre avec KERR et alii[17], que le développement commercial des exosquelettes par des firmes commerciales ne débouche sur un glissement de la médecine réparatrice à une approche basée sur

[13] Dès 1960, le neurophysiologiste J. DELGADO affirmait cette possibilité (voir en particulier son ouvrage : *Physical control of the mind : toward a psychocivilized society*, Harper & Row (New York),1969 [1ère édition],traduction en français : *Le Conditionnement du cerveau et la liberté de l'esprit*, Ch. Dessart (Bruxelles), 1972) : « (mes travaux) *amènent à la conclusion déplaisante que les mouvements, les émotions, et l'humeur, peuvent être contrôlés par des signaux électriques et que les humains peuvent être contrôlés comme des robots en appuyant sur des boutons* » *« Nous sommes seulement au début de notre compréhension de la stimulation électrique du cerveau, mais nous savons qu'elle peut retarder un battement cardiaque, bouger un doigt, inspirer un mot dans la mémoire [les pensées], et provoquer des sensations* ». Sur ce point, voir les travaux de la société de E. MUSK, NEURALINK : la greffe de capteurs dans le cerveau d'un singe lui permettant de contrôler mentalement un ordinateur. Un projet d'implantation de micro-électrodes chez une personne paralysée pour cause de lésion de la moelle épinière a été soumis à la *Food and Drug U.S. Administration* pour autorisation.

[14] On signale en particulier la main bionique (Bionicohand) qui permet à la personne handicapée de retrouver toutes les fonctionnalités du bras. Sur cette création disponible en open source, voir le site https://bionico.org/,

[15] On cite souvent le cas en 2013 du petit Kaiba Gionfriddo, qui souffrait d'une maladie appelée trachéobronchomalacie et risquait le blocage des bronches. Des médecins américains ont créé une prothèse biorésorbable *via* impression 3D, qui a permis d'élargir la trachée et les poumons affaissés d'un nouveau-né. Sur cette opération, lire l'article du médecin G. GREEN, « Bioresorbable Airway Splint Created with a Three-Dimensional Printer », *New England Journal of Medecine*, 23 mai 2013.

[16] Le logiciel In Moov est présenté comme suit sur le site in Moov : « *Gael Langevin est un sculpteur et designer Français. Il travaille pour les plus grandes marques depuis plus de 25 ans. InMoov est son projet personel qu'il a initialisé en Janvier 2012 en tant que première prothèse Open source imprimée en 3D, qui donnera naissances à des projets comme Bionico, E-Nable, et beaucoup d'autre. InMoov est le premier robot Open Source à taille humaine entièrement imprimé en 3D.*

[17] A cet égard, I. KERR et alii, déjà cité, p. 262

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

l'augmentation de l'humain, réservée à ceux qui peuvent se permettre de faire « *better and well* ». Depuis, la technologie du 3D a envahi d'autres domaines de la santé, en particulier celui de la médecine régénératrice. Ainsi, on parle de création de cellules souches grâce à un crayon : le BioPen et de régénérescence de tissus humains[18]. Enfin, la 3D sert également à la fabrication de médicaments dont les caractéristiques permettent une déglutition plus facile pour certaines catégories de patients[19].

6. L'invasion des robots – L'invasion de robots dits intelligents dans le secteur des soins de santé est une autre dimension de l'utilisation de l'IA. Sans être complet[20], citons les catégories suivantes : premièrement, les robots chirurgicaux (comme le célèbre robot « da Vinci »[21]), aident les chirurgiens dans les opérations de la prostate ou d'hystérectomies, en permettant une détection et des gestes plus précis ; depuis certains robots opèrent sans intervention du praticien de l'art de guérir, ainsi le robot STAR[22] est capable de transplanter un intestin de cochon de manière purement automatisée. En deuxième lieu, les pharmacies utilisent des robots comme Script PRO, Robot RX et RIVA pour la fabrication automatique de médicaments. Grâce à des robots, et de manière totalement automatisée, les hôpitaux vitrifient les embryons, opèrent des prises de sang et veillent à une désinfection totale et totalement automatisée de leurs salles d'opération ou pour la distribution de repas, la surveillance des patients, etc. En troisième lieu, on citera les robots dits sociaux, destinés à accompagner voire surveiller le patient, mais également à lui prodiguer des soins et à suivre son état de santé. Il s'agit, entre autres, de *« robots animateurs » en maison de retraite, destinés à stimuler les résidents sur le plan cognitif ou à les « divertir », robots humanoïdes qui interagissent avec des enfants en pédiatrie ou en pédopsychiatrie, « robots d'accueil » entraînés à dialoguer avec les patients et à détecter leurs émotions (!) pour adapter leur discours, coaches virtuels, agents conversationnels en santé mentale, etc.* Ces robots peuvent prendre une forme humanoïde ou représenter un animal de compagnie et le patient peut tisser avec ces objets une relation émotionnelle. Ils facilitent le suivi à domicile, dans la mesure où ils peuvent à distance de l'hôpital détecter des faiblesses ou des incidents de santé et, dans ces cas, prévenir le dispensateur de soin. A cet égard, on cite souvent le robot d'assistance thérapeutique PARO qui cumule l'ensemble de ces fonctions[23].

[18] En particulier, les avancées de POIETIS (https//poietis.com), une spin-off de l'Inserm et de l'université de Bordeaux "*Poietis mission is to provide solutions leveraging a proprietary, innovative Next-Generation Bioprinting platform and bring Tissue Engineering therapies to patients. On the basis of its expertise in high resolution Laser-Assisted Bioprinting, Poietis has developed the Next-Generation Bioprinting (NGB) platform. This modular platform aims to give tissue engineers and researchers greater freedom in the choice of biomaterials and hydrogels and greater versatility in their research and development. Poietis brings to the market two bioprinters based on Next-Generation Bioprinting platform. NGB-R Bioprinter is commercialized for research applications. NGB-C Bioprinter is a clinical-grade, GMP-compliant system dedicated to clinical applications and meet the requirements of translational research and challenges of industrial manufacturing of implantable tissues.*"

[19] « Autorisé en 2015 par la Federal Drug Administration, le premier médicament imprimé en 3D est commercialisé aux États-Unis en avril 2016 par la société Aprecia qui a l'exclusivité pour l'industrie pharmaceutique d'une technique brevetée par le MIT. » (Wikipédia, v° 3D)

[20] Ces différents exemples sont tirés de l'article de I. KERR et alii, *op. cit.*, p. 263 à 265

[21] En juillet 2000, puis en juin 2001, la *Food and Drug Administration* (FDA) autorise l'utilisation du *Da Vinci* aux États-Unis pour un certain nombre d'opérations : cholécystectomie, prostatectomie

[22] Pour une description du fonctionnement de STAR, voir le site : https://www.eedesignit.com/star-the-smart-tissue-autonomous-robot/

[23]. A ce propos, la présentation du Robot (PARO Therapeutic Robot (parorobots.com) "*PARO is an advanced interactive robot developed by AIST, a leading Japanese industrial automation pioneer. It*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

***7. Big Data* Analytics** – Les *applications :* L'introduction signalait par ailleurs l'importance de pouvoir disposer de vastes bases de données structurées, centralisées ou non et permettant aux logiciels d'intelligence artificielle, une fois testés sur des bases de données réduites, de pouvoir croiser les données au fur et à mesure de leur collecte à partir de lieux distincts[24] et de procéder dès lors à des applications d'intelligence artificielle de type *machine learning.* En ce qui concerne ces mégadonnées, l'exemple d'ImageNet, base de données de reconnaissance faciale[25], est souvent cité. Cette mégadonnée contient 1.200.000 images appartenant à 1000 classes différentes détaillées dans *« ImageNet : A Large-Scale Hierarchical Image Database »*[26] et *« Construction and Analysis of a Large Scale Image Ontology »*[27]. Si Image Net est une *big data* ouverte à de nombreuses finalités en dehors de la médecine, comme la recherche de criminels ou la reconnaissance automatique d'employés, d'autres mégadonnées spécialisées existent dans le secteur de la santé. Un article récent[28] liste ainsi 18 domaines dans lesquels la constitution de *big data* existe ou est envisagée, de manière à permettre des « *big data analytics* » : ainsi, une base de données offrant la possibilité de prédire de manière continue le nombre d'entrées à l'hôpital, ce qui permet d'améliorer la gestion du personnel ; celle destinée à l'alerte en temps réel pour l'intervention auprès d'un patient par l'utilisation de données collectées sur des milliers de patients[29] ; les bases de données relatives à la prévention d'abus d'opioïdes[30], à la lutte contre le cancer en

allows the documented benefits of animal therapy to be administered to patients in environments such as hospitals and extended care facilities where live animals present treatment or logistical difficulties : PARO has been found to reduce patient stress and their caregivers ; PARO stimulates interaction between patients and caregivers ; PARO has been shown to have a Psychological effect on patients, improving their relaxation and motivation ; PARO improves the socialiazation of patients with each other and with caregivers. PARO has five kinds of sensors : tactile, light, audition, temperature, and posture sensors, with which it can perceive people and its environment. With the light sensor, PARO can recognize light and dark. He feels being stroked and beaten by tactile sensor, or being held by the posture sensor. PARO can also recognize the direction of voice and words such as its name, greetings, and praise with its audio sensor. PARO can learn to behave in a way that the user prefers, and to respond to its new name. For example, if you stroke it every time you touch it, PARO will remember your previous action and try to repeat that action to be stroked. If you hit it, PARO remembers its previous action and tries not to do that action. By interaction with people, PARO responds as if it is alive, moving its head and legs, making sounds, and showing your preferred behavior. PARO also imitates the voice of a real baby harp seal."

[24] Sur ces *big data* et leurs utilisations en médecine, lire notamment, W. NICHOLSON, « Artificial Intelligence in Health care – Applications and legal issues », *TheSciTechLawyer*, 2017, vol. 14, p. 9 et s. « *Big data as a phenomenon is characterized by the "three Vs" of volume (large quantities of data), variety (heterogeneity in the data), and velocity (fast access to the data). In medicine, the data come from many sources : electronic health records, medical literature, clinical trials, insurance claims data, pharmacy records, and even information entered by patients into their smartphones or recorded on fitness trackers.*" Cf. également, T. CHARTIER, « Vertige, Over the seven V's of Big Data », *The Journal of corporate Accounting and Finance*, 2016, p. 81 et 82

[25] On en épingle d'autres : ainsi celle de Facebook : *Deepface* et celle plus récente et très contestée de la société Clearview.

[26] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li and L. Fei-Fei, *ImageNet : A Large-Scale Hierarchical Image Database. IEEE Computer Vision and Pattern Recognition (CVPR), 2009.*

[27] J. Deng, K. Li, M. Do, H. Su, L. Fei-Fei, *Construction and Analysis of a Large Scale Image Ontology. In Vision Sciences Society (VSS), 2009*

[28] S. DURCEVIC,"18 Examples of Big Data Analytics In Healthcare That Can Save People", *Business Intelligence*, Oct 21st 2020

[29] L'auteure cite ainsi en ce qui concerne le suivi des asthmatiques, la base de données ASTHMAPOLIS : "*Another example is that of Asthmapolis, which has started to use inhalers with GPS- enabled trackers in order to identify asthma trends both on an individual level and looking at larger populations. This data is being used in conjunction with data from the CDC in order to develop better treatment plans for asthmatics.*"

[30] Idem, "*Using years of insurance and pharmacy data, Fuzzy Logix analysts have been able to identify 742 risk factors that predict with a high degree of accuracy whether someone is at risk for abusing opioids."*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

rassemblant toutes les données récoltées par les hôpitaux, les biopsies des patients et le séquençage génétique des tissus tumoraux[31]… Dès 2018, la Commission prônait la mise en réseaux des bases de données souvent développées au niveau national comme des bio-banques, des bases de données d'images de diagnostic ou génétiques, etc.[32].

Il existe nombre d'obstacles à la création de ces bases de données : l'incompatibilité des systèmes de gestion des données entre acteurs, l'absence de standards européens de qualité de fiabilité et de sécurité, la nécessité déontologique de respecter la confidentialité des données et, *last but not least*, la concurrence entre praticiens de l'art de guérir soucieux de garder le privilège que leur accorde l'information dont il dispose et qu'ils n'entendent pas partager ajoutant en outre à l'appui de leur refus, la protection par le droit de la propriété intellectuelle[33]. On sait que dès 2019, la Commission européenne émettait une recommandation relative au format et donc à l'interopérabilité des dossiers électroniques de santé[34]. L'article 11 de la recommandation en précise le champ d'application : « *Les États membres devraient prendre des mesures pour faire en sorte que les domaines d'information sur la santé ci-après, retenus en tant que domaines de référence, fassent partie d'un format européen d'échange des dossiers de santé informatisés : a) dossier des patients ; b) ordonnance électronique/dispensation électronique ; c) résultats de laboratoire ; d) imagerie médicale et rapports y afférents ; e) rapports de sortie de l'hôpital. L'échange transfrontalier d'informations devrait*

[31] Idem, "*in order to make these kinds of insights more available, patient databases from different institutions such as hospitals, universities, and nonprofits need to be linked up. Then, for example, researchers could access patient biopsy reports from other institutions. One of the potential big data use cases in healthcare would be genetically sequencing cancer tissue samples from clinical trial patients and making these data available to the wider cancer database.*" L'exemple d'une base de données en matière de détection et de suivi des cancers du poumon est ainsi souvent cité.

[32] "*The Commission intends step up coordination between authorities across the EU to implement the secure exchange of genomic and other health data in order to advance research and personalised medicine. By combining sequenced genomic data and other medical data, physicians and researchers can get a better picture of disease in a particular individual and determine the most appropriate treatment for that individual. This should be based on a transparent system of governance, with the aim of linking national and regional banks of "-omics"44 data, biobanks and other registries across the EU. The initial goal of this coordination is to provide access to at least 1 million sequenced genomes in the EU by 202245, and then to a larger prospective population-based cohort (beyond sequenced genomes) of at least 10 million people by 2025. This will integrate molecular profiling, diagnostic imaging, lifestyle (in particular risk factors) ; microbiological genomics and environmental data as well as links to electronic health records. It will also build on "digital patient" predictive approaches based on computer modelling, simulations and artificial intelligence. Ultimately, it will help to lay the foundation for developing a reference map (atlas) of all human cells, with a view to analyse human tissues and organs by state-of-the-art methodologies, and to compare and understand changes during disease.*" (EU Commission, Communication on enabling the transformation of health and care in the Digital Single Market, COM(2018)233 final, p. 8). A ce propos, les ERIC (European Research Infrastructure Consortium) créés sous l'impulsion de la Commission européenne qui ont pour but de mettre sur pied des infrastructures communes de recherches, dans des secteurs non marchands. On note l'infrastructure créée en 2014 dans les domaines de la recherche en matière de biobanques et d'analyses de biomolécules (BBMRI ERIC).

[33] En particulier, en Europe, la protection "*sui generis* » des bases de données consacrée par la directive 96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données. Il est à noter que la CJUE dans un arrêt récent (3 juin 2021, Aff. C-762/19, CV Online Lartvia SIA c. Melons SIA) a fortement réduit cette protection en conditionnant l'existence d'un droit sui generis à la preuve d'un risque de non amortissement de l'investissement consenti pour la création de la base de données, cette interprétation permettra certaines extractions et réutilisations de contenus de la base de données, ce qui indéniablement favorisera l'innovation médicale.

[34] EU Commission, RECOMMANDATION (UE) 2019/243 DE LA COMMISSION du 6 février 2019 relative à un format européen d'échange des dossiers de santé informatisés, JOUE, L39/18, 11 février 2019. Sur la situation dans différents pays, lire la thèse de G. VERHENNEMAN, *The patient, Data Protection and Changing Healthcare Models*, KUL Centre for IT and IP Law Series, Intersentia, 2021, p. 33e t s.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

avoir lieu dans le respect des normes de référence, des spécifications d'interopérabilité et des profils en fonction du domaine d'information sur la santé figurant en annexe. »

Par ailleurs, le besoin de permettre l'innovation médicale, la recherche en la matière et d'obtenir de meilleurs soins pour le patient, amène les autorités à encourager le partage des données afin de permettre ces vastes bases de données. Cet enthousiasme en faveur de la création de vastes bases de données de santé publiques accessibles en particulier au monde de la recherche exige cependant une préalable instruction sur le respect de la vie privée des patients mais également des professionnels de santé dont l'activité est « trahie » par la mise en commun de toutes ces données. Dans ses recommandations, qui font suite à son Livre Blanc sur « *Le patient à l'heure des data, des algorithmes et de l'intelligence artificielle* », la recommandation n° 24 rappelle que l'intérêt général, poursuivi par de telles mises en commun, ne peut éluder les règles de protection des données et de secret médical : « *L'exploitation des données massives présente un intérêt majeur, tout particulièrement en matière de santé publique. La plupart des pays occidentaux se sont engagés dans un mouvement d'ouverture des données, « open data ». La France suit cette voie avec la prudence nécessaire que le CNOM accompagne par ses contributions et sa présence dans l'Institut national des données de santé. Le CNOM rappelle que la préservation du secret médical couvrant les données personnelles de santé doit être appliquée aux traitements des données massives et que leur exploitation ne doit pas permettre l'identification d'une personne, au risque de conduire à des discriminations. La loi a établi des règles juridiques portant sur les autorisations d'accès aux bases publiques et aux traitements de données qu'elles contiennent. Ces règles doivent être confortées par leur traduction dans le droit pénal avec des sanctions à hauteur de l'interdit fondateur d'intrusion dans la vie privée et dans un système d'information.* ». Enfin, on note que dans le domaine médical, les collections de données peuvent faire l'objet de recommandations venant du milieu professionnel lui-même, telles que celles de *l'International Collaboration on Cancer Reportings*[35]

8. Des big data... à la recherche scientifique – Ainsi, la constitution au sein des administrations de vastes banques de données dont les ressources pourraient servir l'intérêt de la recherche médicale[36] requiert nos premières réflexions. Il est certain que l'Etat est le premier client de la transformation numérique et en particulier des ressources offertes par l'intelligence artificielle pour fixer sa propre politique de santé publique, mais également de gouvernance et de financement du secteur de la santé. Il est largement tributaire de la production de données de santé et de bien-être issues de ses citoyens pour construire cet « écosystème de la donnée » qui alimentera l'intelligence artificielle. Son rôle ne s'arrête pas là, dans la mesure où son éco-système permet

[35] Voir la liste de publications présente sur le site http://www.iccr-cancer.org.

[36] C'est le sens de la politique européenne de création de vastes biobanques et bases de données génétiques : Lire sur ce point, J. STARKBAUM and U. FELT, « Negotiating the reuse of health-data : Research, Big Data, and the European General Data Protection Regulation », in *Big data and Society, July-Dec. 2019, p. 1-12 : "The trend for bigger data in omics research led to the ongoing integration of European biobanks around the turn of the last millennium (Rial-Sebbag and Cambon- Thomsen, 2015). The Biobanking and Biomolecular Resources Research Infrastructure – European Research Infrastructure Consortium (BBMRI-ERIC), a major EU biomedical infrastructure, was gradually developed over the course of the last two decades and inaugurated in 2013. Its declared aim is to improve cooperation between biobanks and other partners (e.g. from policy and industry) and thus promote scientific research across Europe. In 2015, more than 500 European biobanks were part of this EU infrastructure. »*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

d'alimenter les chercheurs et laboratoires de recherche qui trouvent dans les bases de données collectées à des fins publiques, un matériau essentiel pour la mise au point de médicaments ou de dispositifs de santé[37] mais également pour une meilleure connaissance des patients.

Les recherches sur « *les systèmes informatisés complexes sont en quelque sorte le nouvel eldorado de la recherche et de la clinique médicale* »[38]. C'est en particulier dans le domaine de la recherche médicale que les outils d'intelligence artificielle s'avèrent le plus prometteur : ainsi le projet français DYNAMO qui ambitionne de déceler de manière précoce les personnes atteintes de la maladie d'Alzeihmer[39]. Point commun à tous ces outils, ils vivent et n'ont de sens qu'alimentés par de vastes bases de données. Les sources capables d'alimenter ces bases de données sont nombreuses (voir déjà, *supra,* n° 4) : en premier lieu figurent les bases de données médico-administratives provenant de l'application des lois de sécurité sociale assurant le remboursement des actes médicaux[40], mais au-delà, elles sont générées par l'activité des professionnels de santé dans le cadre ou non de programmes de recherche ou d'expérimentations de dispositifs médicaux ou de soins de santé[41] ; enfin, elles proviennent des patients eux-mêmes qui sont invités dans le cadre de leurs parcours de santé à confier leurs données ou dont les données échangées sur des plateformes (voire réseaux sociaux) peuvent être collectées et servir aux recherches médicales[42]. Dans le cadre de sa proposition de

[37] Ainsi, le très controversé accord entre la National Health Institute anglais et Deep Mind filiale de Google. Sur cet accord, Julia Powles et Hal Hodson, « Google DeepMind and Healthcare in an Age of Algorithms », *Health and Technology* 7, n° 4 (1 décembre 2017) : 351-67, https://doi.org/10.1007/s12553-017-0179-1.

[38] Michèle STANTON-JEAN, « Les systèmes informatisés complexes en santé sous le regard de la bioéthique et des droits de l'homme », dans Christian HERVÉ, Michèle STANTON-JEAN et Éric MERTINENT (dir.), *Les systèmes informatisés complexes en santé. Banques de données, télémédecine : Normes et enjeux éthiques*, coll. « Thèmes et commentaires » Paris, Dalloz, 2013, p. 5.

[39] Voilà comment le projet DYNAMO est présenté par le Livre Blanc de la CNOM déjà cité (p. 43) : « *Ce projet repose sur notre capacité à collecter et exploiter des données issues de milliers de personnes atteintes de maladie d'Alzheimer ou à risque. Ces big data, confrontées les unes aux autres dans des modèles mathématiques dynamiques très précis, pourraient révéler les biomarqueurs les plus fiables de la maladie d'Alzheimer et les mécanismes à l'oeuvre dans celle-ci », expliquent le professeur de neurologie Harald Hampel (ICM) et le spécialiste de la modélisation mathématique des données de neuro-imagerie, Stanley Durrleman (INRIA). L'objectif consiste à créer un outil informatique accessible aux médecins, capable de diagnostiquer au plus tôt la maladie et de produire un pronostic d'évolution personnalisé pour chaque patient. Mais les chercheurs verraient bien ce modèle dupliqué par la suite… « Il s'agit de créer un outil inédit, permettant de mettre les big data au service de notre santé. Développé dans un premier temps pour mieux comprendre et donc combattre la maladie d'Alzheimer, ce modèle pourrait être le point de départ d'un changement de paradigme dans le traitement de plusieurs affections neuro* »

[40] « *D'ici 2019, notre système national des données de santé (SNDS) rassemblera 450 téraoctets (1012 octets) d'informations stratégiques rassemblées dans une seule base, alors qu'aux États-Unis ce volume s'élève déjà à 150 exa-octets (1018 octets). Cette avancée permettra d'analyser et améliorer la santé de la population notamment en ce qui concerne les patients souffrant de maladies chroniques.* « (CNOM, *Médecins et patients dans le monde des data, des algorithmes et de l'intelligence artificielle*, *Livre Blanc,* déjà cité__,__ p. 13)

[41]. « *Dans des centres hospitaliers universitaires pionniers sur le sujet, riches de millions de dossiers patients numérisés, les entrepôts de données facilitant la constitution de cohortes et la recherche translationnelle se mettent en place depuis peu. Si l'application des big data en génomique n'occupe encore qu'une petite place parmi les méthodes de recherche et traitement des maladies, le lancement du Plan France Médecine génomique 2025 a prévu, d'ici à 2020, le déploiement d'un réseau de 12 plateformes de séquençage à très haut débit. Les deux premières plateformes pilotes viennent d'être sélectionnées et devraient commencer à fonctionner fin 2018. Ce Plan a aussi annoncé la mise en place d'un centre national de calcul intensif capable de traiter et d'exploiter le volume de données qui seront générées par les plateformes et d'offrir analyses in silico et outils d'aide à la décision ; »* CNOM, « *Médecins et patients dans le monde des data, des algorithmes et de l'intelligence artificielle*, *Livre Blanc,* déjà cité__,__ p. 13.

[42] Voir notamment l'expérience RENALOO qui collecte et traite des données provenant de telles sources : « *Les associations de patients, et les patients eux-mêmes, sont aussi des producteurs d'informations*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

Règlement appelé le « *Data Governance Act* »[43], la Commission européenne pousse les citoyens à consentir au transfert et à l'utilisation de leurs données médicales à des fins de recherche en matière de santé et ainsi à accélérer le développement d'innovations tant pharmaceutiques que de soins. Nous reviendrons sur ce qu'il est convenu d'appeler le « Data altruisme ».

9. La médecine personnalisée et les données génomiques : Les secondes réflexions portent sur l'avènement de la médecine personnalisée, réclamée, dès 2002, comme un droit par la « Charte européenne des patients »[44]. Le document stratégique de la Commission européenne[45] y voit un argument en faveur de l'utilisation de l'intelligence artificielle : « *Personalised medecine will better respond to the patients' needs by enabling doctors to take data-enabled decisions. This will make it possible to tailor the right therapeutic strategy to the needs of the right person at the right time, and/or determine the predisposition to disease and/or deliver timely and targeted prevention.*" Cette médecine personnalisée[46] entend suivre le patient de manière continue tout au long de sa vie et entend, par ailleurs, s'appuyer sur l'utilisation des données génétiques des personnes. A cet égard, on connaît l'ambition du « Projet de génome humain »[47], qui entend établir des liens entre des variations du DNA et des risques de maladie. Comme le note un groupe de chercheurs[48], le terme « médecine personnalisée » re-

utiles. Pour avoir vécu leur ressenti, leur appréciation sur la qualité de vie et la qualité des traitements, cela peut être utile pour les agences sanitaires qui évaluent les produits de santé, pour les soignants qui cherchent à améliorer leurs conditions d'exercice et être à l'écoute des besoins des patients ce qui est essentiel.

Renaloo est une association qui existe depuis le début sur un format très digitalisé et fait ce pari qu'en collectant les données qui sont issues du monde des patients et en les exploitant, on peut améliorer la recherche, la coordination des soins et le rapport au patient. C'est dans cet objectif que nous développons aussi des plates-formes digitales… Renaloo considère que toutes les informations que nous pouvons recueillir à partir des réseaux sociaux indiquent quelque chose sur ce que ressentent les patients et c'est utile pour l'évaluation d'un médicament, d'un nouveau protocole, sur des précautions à prendre en termes de contraception, de grossesse, de médicaments tératogènes. On peut facilement faire une enquête patient qualitative à partir des réactions des patients. Certes cela ne répond pas à des méthodologies scientifiques de sondage, mais cela dit quelque chose et qui permet d'apporter un argumentaire étayé. » (Intervention de M. LEO, lors du débat initié par la CNOM à propos du Livre Blanc cité note précédente__, Débats de l'Ordre__, janvier 2018, document déjà cité, p. 13)

[43] Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la gouvernance européenne des données (acte sur la gouvernance des données), Bruxelles, le 25.11.2020, COM(2020) 767 final 2020/0340(COD)

[44] Active Citizens' Network, *European Charter of patient's Rights,* Rome 15 nov. 2002, recommendation n° 12.

[45] Communication from the Commission to the EU Parliament, the Council and the Committee of Regions, « *A European Strategy for Data*", COM(2020) 66, 19 février 2020, p ?.2 ;

[46] A cet égard, parmi de nombreux auteurs, lire L. HOOD et S. FRIEND, « Predictive, personalized, preventive, participatory (P4), *8 Nature, Reviews, Clinical ontology,* 184 et s. Ces auteurs insistent sur le fait que cette médecine personnalisée à la fois préventive et prédictive doit en même temps s'appuyer sur la participation du patient. D'où l'appellation Médecine P4.

[47] Ce projet débuté en 1986 repose sur la collaboration de nombreux laboratoires de recherche et cherche à séquencer de manière complète le génome humain. Ce séquençage complet a pu être obtenu en 2020. Sur ce projet, lire la présentation par Britannica (www.britannica.com/event/Human-Genome-Project) : « *Human Genome Project (HGP), an international collaboration that successfully determined, stored, and rendered publicly available the sequences of almost all the genetic content of the chromosomes of the human organism, otherwise known as the human genome. The Human Genome Project (HGP), which operated from 1990 to 2003, provided researchers with basic information about the sequences of the three billion chemical base pairs (i.e., adenine [A], thymine [T], guanine [G], and cytosine [C]) that make up human genomic DNA (deoxyribonucleic acid). The HGP was further intended to improve the technologies needed to interpret and analyze genomic sequences, to identify all the genes encoded in human DNA, and to address the ethical, legal, and social implications that might arise from defining the entire human genomic sequence."*

[48] D.LEVY, G. Mc DOUGALL, T. PILLARI, et alii, *The new science of personalised medecine : translating promise into practice,* 2009, cite par G. VERHENMAN, *op. cit.*, p. 41.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

groupe *« products and services that leverage the science of genomics and prorteomics (directly or indirectly) and capitalise on the trens toward wellness and consumerism to enable tailored approaches to prevention and care."* La diminution des coûts en ce qui concerne l'analyse du bagage génétique des personnes, l'irruption sur le marché d'entreprises offrant cette analyse et, parfois, les conseils de santé corrélés à cette analyse, poussent deux tendances fortes de l'évolution du secteur de la santé, favorisées par les technologies de l'intelligence artificielle : premièrement, le passage d'une médecine curative à une médecine préventive, voire prédictive, l'évolution d'un concept de la santé réparatrice à celui d'une santé 'bien-être' et finalement, avec l'irruption de nouveaux services rendus par des acteurs extérieurs à la santé, une tendance à la « consumérisation » du secteur. Le chapitre II analyse cette irruption de nouveaux acteurs dans le champ de la santé ainsi élargi.

Les récentes innovations connues sous le nom de CRISP Case 9[49] illustrent une autre utilisation possible de la connaissance des données génomiques d'une personne, à savoir la possibilité de pouvoir modifier le génome d'une personne. Après la mise sur le marché d'animaux et de plantes modifiés par édition du génome, après le lancement de plusieurs essais cliniques sur des cellules somatiques, une équipe chinoise dirigée par le Dr He Jiankui a annoncé, le 28 novembre 2018, la naissance de jumelles humaines dont le génome a été modifié par la technologie CRISPR dans le but de les rendre insensibles à l'infection par le VIH. Sans doute, cette première a fait l'objet de vives critiques des milieux éthiques de la recherche médicale, mais les potentialités liées à cette innovation chirurgicale sont pleines de promesses.

2 De quelques questions éthiques et juridiques relatives à la médecine de demain

10. La « datafication » des patients et la déshumanisation des soins – La réduction de la personne à « ses » données caractérise les traitements utilisés par nombre de système d'intelligence artificielle et soulève la question de la dimension empathique des soins de santé, au moment où le professionnel risque de ne plus communiquer avec son patient que par données interposées. Lorsqu'une telle réduction est à la base de décisions ou de propositions de décision, qui, dans le contexte où elles sont émises apparaissent comme difficilement discutables par la personne responsable de la décision vis-à-vis d'un patient, elle est de même contraire à la dignité humaine qui exige la possibilité pour chacun de pouvoir réclamer non seulement l'explication de la décision prise à son encontre, mais également celle de pouvoir la contester et d'être entendue pour ce faire par une personne humaine capable de réformer la décision prise à son encontre. Comme l'écrit A. ROUVROY[50], *« cette construction numérique de la réalité façonne une « mémoire du futur », mémoire éminemment plastique, actualisée en temps réel, « objective », non située, dont tous les éléments sont en permanence et immédiatement disponibles. Cette « mémoire du futur » permet une nouvelle ma-*

[49] Comité d'éthique de l'INSERM, *Saisine concernant les questions liées au développement de la technologie CRISPR Cas9*, Etude disponible sur le site http://www.inserm.fr/sites/default/files/2017-10/Inserm___Saisine_ComiteEthique_Crisp-Cas9_Fevrier2016.pdf

[50] A. ROUVROY, « L_'Homo juridicus_ est-il soluble dans les données ? », in *Droits, normes et libertés dans le cybermonde, Liber Amicorum Yves Poullet,* E. DEGRAVE et alii (éds), Cahier du CRIDS, n° 43, 2018, p. 417- 443.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

nière de « gouverner » à partir du monde (numérisé) lui-même, suivant une logique purement inductive (de corrélations statistiques), et à travers des stratégies de préemption consistant à structurer a priori le champ de perception et d'action possible des individus – en fonction de ce qu'ils pourraient faire ou vouloir – et ce tout en se dispensant tant d'une évaluation individualisée des personnes et des situations, que de toute intervention directe sur l'actuel. ».

L'article 11 de la loi française relative à la bioéthique[51], répond imparfaitement certes mais cependant de manière partielle à cette préoccupation en garantissant l'information du patient et la présence d'une intervention humaine en cas d'utilisation des traitements algorithmiques[52]. Certes, on souligne d'emblée les limites de ces garanties : l'information délivrée au patient sur le recours à l'IA suppose un médecin capable d'expliquer le traitement algorithmique opéré par le système. Par ailleurs, la loi n'exige pas le consentement du patient qui, dès lors, ne peut s'opposer au recours. Enfin, à moins que le fabricant puisse *by design* prendre toutes les dispositions pour que le médecin conserve la maitrise de l'outil (« *Human at the command* »), on peut craindre que le principe de la garantie humaine soit difficile à mettre en œuvre par un praticien peu aguerri au fonctionnement de l'IA et qui, dès lors, risque alors de simplement valider son résultat,

11. Un patient prévisible – « *Nous sommes maintenant capables*, écrit B. SCHRODER[53], *de résoudre de toutes nouvelles classes de problèmes, telles que la reconnaissance d'image ou la transcription de la voix. Nous pouvons prédire des événements non modélisables. Par exemple, Cornell University détecte la survenance de l'état dépressif de patients bipolaires en analysant les changements dans la frappe de messages sur l'écran d'un smartphone (BOKAI Z. & alii. KDD'17 Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining Pages 747-755, ACM). Un algorithme de Microsoft prévoit un diagnostic futur de cancer du pancréas ou de poumon par l'analyse de l'historique des mots clés entrés dans un moteur de recherche (PAPARRIZOS J. & alii, "Screening for Pancreatic Adenocarcinoma Using Signals From Web Search Logs : Feasibility Study and Results" Journal of Oncology Practice 12, no. 8 (August 01, 2016) 737-744.).* ». Ces craintes d'une prédiction de notre santé future justifient pleinement des réglementations interdisant l'utilisation en particulier de données génétiques par certaines professions, telles les banquiers ou les assureurs[54].

[51] Pour une analyse globale sur le projet tel que déposé à l'Assemblée nationale le 24 juillet 2019, V., B. Bévière-Boyer, « Numérique en santé : le projet de loi relatif à la bioéthique a accouché d'une souris », *in* N. Nevejans (dir.), *op. cit.*, p. 243-256.

[52] Ce texte a pour objet d'introduire un nouvel art. L. 4001-3 dans le CSP : « *I. – Lorsque, pour des actes à visée préventive, diagnostique ou thérapeutique, est utilisé un traitement algorithmique dont l'apprentissage est réalisé à partir de données massives, le professionnel de santé qui décide de cette utilisation s'assure que la personne concernée en a été informée au préalable et qu'elle est, le cas échéant, avertie de l'interprétation qui en résulte.*
I bis. – Aucune décision médicale ne peut être prise sur le seul fondement d'un traitement mentionné au I.
II. – Un principe de garantie humaine s'applique à ces traitements algorithmiques. La mise en œuvre de ce principe est notamment assurée par le fabricant dans les conditions prévues dans le cadre de la mise sur le marché du traitement algorithmique. »

[53] B. SCHRODER, *Vie Privée, transparence et démocratie,* Actes du Colloque du REHNAM, Namur le 28 novembre 2019, Y. Poullet (éd.), Cahier du CRIDS, n° 50, 2020.

[54] Ainsi, la loi belge sur les assurances, modifiée récemment, le 4 décembre 2020, prévoit (article 4.2) : « *Lors de la conclusion du contrat visé à l'article 46/1, le refus du candidat assuré d'acquérir ou*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

Ainsi, l'IA, aux risques de biais et d'erreurs[55], permet non seulement de mieux appréhender ce que nous avons fait, de nous reconnaître mais également de se tourner vers l'avenir et de prédire nos comportements futurs. Elle nous rend, jusqu'à un certain point du moins, transparents et prédictibles au moment même où la complexité du fonctionnement des algorithmes qui constituent le système, la richesse des données sur lesquelles ils travaillent (quelles corrélations ? entre quelles données ? avec quels poids ?) rendent le système non transparent, certes pour la personne concernée, mais également pour l'exploitant de cet instrument lorsqu'il s'agit de systèmes dits de '*deep learning'* ou d'apprentissage profond.

12. Un patient augmenté – Au-delà, l'irruption du numérique dans la santé permet d'augmenter les capacités de l'homme *via* des implants corporels permettant par exemple, de décupler la mémoire, de les relier à des intelligences artificielles, présents dans des ordinateurs externes, ou de lutter contre la vieillesse ou par des manipulations génétiques. Si on n'y prend garde, ces possibilités nouvelles de soins ouvrent à terme la voie à une humanité à deux vitesses par définition discriminante si l'offre de telles possibilités reste réservée à ceux qui financièrement peuvent se les « offrir ». Dès 2005, le Groupe européen d'éthique des sciences et des technologies nouvelles soulevait la question. Il s'inquiétait en outre des droits de propriété intellectuelle entourant de telles innovations qui risquaient de priver nombre d'acteurs de la possibilité d'avoir accès à de tels progrès. Le financement par la sécurité sociale de l'accès à certaines innovations en matière de santé est sans doute une solution à explorer.

La possibilité de modification ciblée de notre génome est désormais possible grâce à l'utilisation de ciseaux moléculaires qui, selon la technologie CRISP-Cas9, permet d'enlever une partie de l'Adn ou de remplacer une partie défectueuse. Quelle réflexion éthique porter sur les applications de cette technologie ? Quelle posture le droit adopte-t-il face à ces expérimentations ? On invoque l'article 16-4 du code civil français qui sur base des recommandations éthiques de l'UNESCO de 2005 invoque le principe de l'intégrité de l'espèce humaine : « *Nul ne peut porter atteinte à l'intégrité de l'espèce humaine. Toute pratique eugénique tendant à l'organisation de la sélection des personnes est interdite. Est interdite toute intervention ayant pour but de faire naître un enfant génétiquement identique à une autre personne, vivante ou décédée. Sans préjudice des recherches tendant à la prévention et au traitement des maladies génétiques, aucune transmission ne peut être apportée aux caractères génétiques dans le but de modifier la descendance de la personne.* » Cet article invite à distinguer

d'utiliser un objet connecté qui récolte des données à caractère personnel concernant son mode de vie ou sa santé ne peut en aucun cas conduire à un refus d'assurance ni à une augmentation du coût du produit d'assurance » ; (article 5) : « *Aucune segmentation ne peut être opérée sur le plan de l'acceptation, de la tarification et/ou de l'étendue de la garantie sur la base de la condition que le candidat assuré accepte d'acquérir ou d'utiliser un objet connecté qui récolte des données à caractère personnel concernant son mode de vie ou sa santé, accepte de partager des informations récoltées par un tel objet connecté, ni sur la base de l'utilisation par l'assureur de telles informations* ». De manière plus nette encore, le « *Genetic Information Non discrimination Act* « (GINA) américain du 21 mai 2008, interdit l'utilisation de certaines catégories de données génétiques en matière d'emploi et d'assurance. On doit s'attendre à une multiplication de telles réglementations spécifiques.
vu les risques importants de discrimination en matière de santé, d'éducation, d'emploi et d'accès à des services financiers ou d'assurance que représentent les capacités prédictives et décisionnelles de l'IA.

[55] Ainsi, à propos de l'utilisation du système IA d'IBM Watson, l'analyse proposée par M.C. JAKLEVIC, « MD Anderson Cancer Center's IBM Watson project fails, and so did the Jourmnalism related to », Health News Review, 23 février 2017.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

une intervention sur le génome à des fins médicales, c'est-à-dire de soin réparateur (éthique du *care*) sans conséquence pour les générations futures) de celle visant le bien-être supposé de la personne (homme augmenté) ou pratiqué sur l'embryon à des fins de sélection ou d'amélioration de la race. En ce qui concerne la recherche médicale, les frontières sont plus floues. Faut-il admettre ou au contraire interdire l'édition du génome d'un embryon au nom de l'intérêt des générations futures et de l'intérêt thérapeutique qu'il pourrait apporter du fait des résultats de la recherche ? De nombreux rapports récents abordent le sujet[56].

La dignité humaine, c'est-à-dire le respect de chacun comme personne d'égale valeur, implique le respect de notre « identité ». En matière d'édition du génome, le CEI et le COMETS défendent les principes suivants : – « *Encourager la recherche pour évaluer l'efficacité et l'innocuité de la technologie CRISPR dans des modèles expérimentaux et déterminer ainsi la balance bénéfice/risque des applications thérapeutiques, y compris éventuellement sur des cellules germinales et sur l'embryon ; – Évaluer les effets potentiellement indésirables du guidage de gène (« gene drive ») ; – Respecter l'interdiction de toute modification du génome nucléaire germinal à visée reproductive dans l'espèce humaine, et n'appuyer aucune demande de modification de cette interdiction avant que les incertitudes concernant les risques ne soient plus clairement évaluées, et sans qu'une concertation élargie incluant les multiples partenaires de la société civile n'ait statué sur ce scénario ; – Participer à toute initiative nationale ou internationale qui permettra de concilier liberté de la recherche et respect des principes fondamentaux des droits de l'homme.* » Les remarques que nous adressons aux technologies d'implants corporels et d'augmentation des capacités humaines valent bien évidemment également pour les développements de la génétique médicale obtenus à partir des technologies NBIC[57]. Ainsi, les premières techniques de découpage et de construction du génome ou des génomes humains[58] permettent d'envisager l'effacement de certaines déficiences propres à certains êtres humains (le fantasme du gène « criminel ») et la construction de personnalités aux 'meilleurs' bagages génétiques. Outre les questions déjà rencontrées, ces manipulations génétiques soulèvent la question des choix portés par des personnes d'une génération, en ce qui concerne leurs futurs héritiers. Peut-on admettre que ces choix soient imposés aux générations futures ? Par ailleurs, ces technologies entendent modifier parfois en profondeur l'identité humaine. Cette modification acceptée par l'individu ainsi transformé peut-elle imposer à la société de revoir les conséquences des actes posés sous l'ancienne identité ? Ainsi, celui qui a commis un crime et dont le gène criminel a pu être réparé, peut-il exiger une libération et une remise en grâce au nom de son identité nouvelle ? Que ces questions doivent être portées à la discussion générale, qu'elles exigent une réflexion éthique à la

[56] Pour ne citer que la France : Comité d'éthique INSERM, Office parlementaire des choix politiques et scientifiques

[57] A cet égard, le rapport de la National Science Foundation des Etats Unis (NSF) en 2002 qui consacre le concept de NBIC, M. ROCO et W. BAINBRIDGE, *Converging Technologies for Improving Human Performance,* Juin 2002

[58] « *Si la matière est de l'information (codage), le traitement de celle-ci permet de copier le vivant naturel mais aussi de le reprogrammer. Désormais, on 'façonne le monde atome par atome à cette échelle pour laquelle il n'y a pas de différence entre la matière inerte et la matière vivante… Elle permet de modifier le comportement des vivants naturels mais aussi de penser à d'autres formes de vivants que ceux que la nature nous révèle* » (T. MAGNIN, *Penser l'humain au temps de l'homme augmenté,* Albin Michel, 2017, p. 34 et 35).

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

hauteur des défis et risques sociétaux en jeu comme l'affirme le rapport VILLANI[59], un 'contrefort éthique' dirait le recteur GIORGINI[60], et à tout le moins un devoir de précaution, nous paraît évident.

13. Des performances de l'IA et de la dé-responsabilisation des professionnels de santé – Dans un article en voie de publication, Yacine DAQUIN[61] relève que certains systèmes d'intelligence artificielle présentent des résultats meilleurs que ceux des praticiens de l'art de guérir[62]. Il serait alors contraire aux exigences posées par le droit d'une attitude conforme à la diligence attendue du « bon » praticien de l'art de guérir, que soit sanctionnée la prise en considération exclusive des recommandations algorithmiques, lorsque l'algorithme satisfait à des exigences de qualité au cours d'un processus d'évaluation sur lequel nous reviendrons et a fait ses preuves. Sans doute, le respect de telles exigences, le processus d'évaluation et le recueil des preuves doivent-ils s'intégrer dans le contrôle du système d'IA, opéré dès la conception de celui-ci par des représentants des praticiens de l'art de guérir, dans la mesure où on peut difficilement exiger de chaque praticien la connaissance technique qui lui permettrait de juger de manière appropriée. Notons simplement à ce stade que la responsabilité du médecin n'est pas évacuée par l'application d'un régime de responsabilité des concepteurs ou fabricants du système d'IA, il lui reste à devoir s'informer des qualités du système qu'il entend utiliser et, tantôt, systématiquement examiner les résultats

[59] « *Les progrès récents de l'IA dans de nombreux domaines (voitures autonomes, reconnaissance d'images, assistants virtuels) et son influence croissante sur nos vies l'ont placée au centre du débat public. Ces dernières années de nombreuses voix se sont interrogées sur la capacité de l'IA à réellement œuvré pour notre bien-être et sur les dispositions à prendre pour s'assurer que cela soit le cas.*
Ce débat a principalement pris la forme d'une large réflexion sur les enjeux éthiques liés au développement des technologies d'intelligence artificielle et plus largement des algorithmes. En différents endroits du monde, experts, régulateurs, universitaires, entrepreneurs et citoyens discutent et échangent régulièrement sur les effets indésirables, actuels ou potentiels de ceux-ci et les moyens de les atténuer. Placées sous la nécessité d'articuler les potentialités offertes par ces technologies avec le respect de nos valeurs et normes sociales, ces discussions ont logiquement puisé dans le vocabulaire de l'éthique. Elles ont investi l'espace disponible entre ce qui est rendu possible par l'IA et ce qui est permis par la loi pour discuter de ce qui est souhaitable. Or, l'éthique est précisément cette branche de la philosophie qui se consacre exclusivement à l'étude de cet espace en tentant de distinguer le bien du mal, l'idéal vers lequel tendre et les chemins qui nous en éloignent. » (Rapport VILLANI, *op. cit.*, p. 139 et s.)

[60] P. GIORGINI, *La tentation d'Eugénie,* Bayard, 2018 ; p. 322 et s. L'auteur plaide pour une science du « contrefort éthique » qui « *en tant que discipline, appuyée sur la modélisation des systèmes complexes et la théorie des systèmes autopoïétiques, elle tenterait de définir un corpus de concepts et de méthodes permettant de créer une unité épistémologique.* ».

[61] Y. DAQUIN, « Les enjeux éthiques et juridiques de l'intelligence artificielle. Etude à partir d'un cas d'ophtalmologie », article à paraître. L'auteur analyse un système expert utilisé en ophtalmologie, soit le TCO. « *Le dispositif que nous allons étudier est un réseau de neurones à convolution qui a pour objectif d'analyser les images et de les classifier à partir d'une tomographie en cohérence optique (TCO). L'algorithme peut classer les images dans plusieurs catégories : dégénérescence maculaire liée à l'âge (DMLA), une rétinopathie diabétique, drusen ou normal. Les deux premières correspondent à des pathologies, sont la cause majeure de la perte de vue et se soignent avec un inhibiteur du facteur de croissance de l'endothélium vasculaire ou anti-VGEF.* »

[62] Voilà ce que DAQUIN écrit de manière nuancée : « Or, la validation de l'intelligence artificielle repose sur la comparaison avec un *golden standard* supérieur à ce critère comme l'illustre notre étude. En effet, l'algorithme est mis en compétition avec des médecins « dotés d'une expérience clinique significative ». Les résultats de ce concours sont les suivants : le taux d'erreur pondéré de l'algorithme est de 6,6%, celui des médecins est en moyenne de 4,8% (le plus haut taux d'erreur est de 10,50%, le plus bas de 0,40%). De manière générale sur la performance élevée des systèmes de détection de maladies à partir de systèmes d'imagerie médicale comparée à celle des diagnostics des médecins spécialistes, lire Xiaoxuan Liu *et al.*, « A Comparison of Deep Learning Performance against Health-Care Professionals in Detecting Diseases from Medical Imaging : A Systematic Review and Meta-Analysis », *The Lancet Digital Health* 1, n° 6 (1 octobre 2019) : e271-97, https://doi.org/10.1016/S2589-7500 (19) 30123-2.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

donnés par la machine, tantôt, d'une manière ou d'une autre assumer une supervision régulière et attentive du fonctionnement d'une machine certifiée par ailleurs.

Au-delà de cette phase de conception, la question de la responsabilité du professionnel de santé qui utilise un système d'IA est délicate. Peut-on reprocher au médecin d'avoir utilisé un système d'IA ? *Peut-il s'exonérer de sa responsabilité propre et dans quelle mesure peut-il déléguer à une machine, le soin de soigner ou d'établir le diagnostic ?* Sans doute, si le système d'IA choisi ne méritait pas sa confiance, soit par son immaturité, soit au regard de l'incongruité complète des résultats proposés. Dans les deux cas, on peut considérer qu'il est du devoir du médecin de ne pas se satisfaire du résultat proposé par le dispositif d'IA. Et qu'il existe chez lui un devoir réel de vérification de la 'vérité sortie de l'ordinateur', ce qui suppose qu'il ait un minimum de connaissance des paramètres du fonctionnement de la machine, des tests réalisés, de ses performances et des données utilisées. Ce devoir de vérification peut être facilité par l'audit de qualité réalisé par un tiers qui aura pris soin de faire appel à une représentation des professionnels de santé.

Pour reprendre la question sous un autre angle, faut-il exiger l'intervention de l'humain dans toute décision médicale, comme le réclame le Comité national pilote d'éthique du numérique dans son analyse critique du Livre Blanc de la Commission sur l'intelligence artificielle[63] ? « *Le Livre Blanc intègre, à juste raison, la notion d'une « Garantie Humaine de l'intelligence artificielle » (Human Oversight ou Human Warranty). Ce principe a d'ores et déjà fait l'objet de travaux abondants dans le cadre du processus en cours de révision de la loi de bioéthique française sous l'égide du CCNE et des démarches initiées par le CNPEN. Cette idée d'une Garantie Humaine de l'IA est issue d'un mouvement de propositions académiques, citoyennes mais aussi de professionnels de santé. Ce principe a été reconnu dans les avis 129 et 130 du CCNE et dans l'article 11 du projet de loi bioéthique en cours d'examen devant le Parlement français. Cette notion a également été portée dans le cadre des travaux en cours de la task-force sur la régulation de l'IA dans le cadre de l'Organisation Mondiale de la Santé. Le concept de « Garantie Humaine » peut paraître abstrait mais il est, en réalité, très opérationnel. Dans le cas de l'IA, l'idée est d'appliquer les principes de régulation de l'intelligence artificielle en amont et en aval de l'algorithme lui-même en établissant des points de supervision humaine. Non pas à chaque étape, sinon l'innovation serait bloquée. Mais sur des points critiques identifiés dans un dialogue partagé entre les professionnels, les patients et les concepteurs d'innovation. Dans le domaine de la santé, le CCNE a proposé que cette supervision puisse s'exercer avec le déploiement de « collèges de garantie humaine » associant médecins, professionnels paramédicaux et représentants des usagers. Leur vocation serait d'assurer a posteriori une révision de dossiers médicaux pour porter un regard humain sur les options thérapeutiques conseillées ou prises par l'algorithme. L'objectif consiste à s'assurer « au fil de l'eau » que l'algorithme reste sur un développement de Machine Learning à la fois efficace*

[63] Comité National Pilote d'Ethique du Numérique, « Consultation sur le Livre blanc sur l'intelligence artificielle. Une approche européenne », Avis (Comité Consultatif National d'Ethique, 14 juin 2020). P.12 (Disponible à l'adresse suivante : https://www.ccne-ethique.fr/fr/actualites/contribution-du-cpen-dans-le-cadre-de-la-communication-sur-le-livre-blanc-de-la-commission?page=4. Cf. également la prise de position de radiologues : Thibaut Jacques *et al.*, « Proposals for the Use of Artificial Intelligence in Emergency Radiology », *Diagnostic and Interventional Imaging*, 2 décembre 2020, https://doi.org/10.1016/j.diii.2020.11.003. p. 2

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

médicalement et responsable éthiquement[64]. » Cet appel à la garantie humaine n'est-elle pas cependant un vœu pieux dans la mesure où il deviendra de plus en plus risqué pour un professionnel de la santé d'aller à l'encontre de la vérité sortie des algorithmes.

14. De la perte de maîtrise des professionnels de santé au profit de nouveaux acteurs (les medtech) – La mise au point des logiciels d'IA, la mise en place des infrastructures pour obtenir les données nécessaires à leur fonctionnement et pour les traiter par la suite font intervenir des acteurs de plus en plus nombreux et, pour certains, étrangers au monde médical traditionnel[65]. La littérature les qualifie volontiers de « *Medtechs* »[66]. Ces sociétés opèrent souvent comme sous-traitants ou comme auxiliaires du travail des praticiens de l'art de guérir en développant les algorithmes nécessaires au travail médical et, de manière plus large, des dispositifs médicaux ; en mettant au point les robots, en offrant des services de *cloud*, de télémédecine ou de *back up*. Bien souvent les données collectées par le médecin sont recueillies directement ou indirectement, traitées et conservées par des entreprises tierces, qui gèrent à la fois les données mais également les accès aux données tant de base, que celles résultantes du traitement. Nombre de services de téléconsultation, de télé-expertise ou de télé-monitoring peuvent s'exercer en dehors de l'action, de la présence ou de la surveillance d'un médecin[67]. Ainsi un serveur de haute capacité détenu par une entreprise située en dehors du secteur médical analysera les données d'imagerie médicale envoyées par de nombreux hôpitaux de manière à leur appliquer des algorithmes d'intelligence artificielle. On connaît le scandale qu'a entrainé la conclusion de contrats du gouvernement français avec le géant Microsoft pour l'hébergement des données médicales[68]. Comment aborder la situation de ces prestataires techniques qui opèrent

[64] Nous reviendrons sur cette idée d'un contrôle collectif par le milieu des praticiens de l'art de guérir, plus efficace et réaliste qu'un contrôle singulier par chacun de ces praticiens.

[65] Emmanuel PAVAGEAU et Hubert MARCUEYZ, « Rôle de l'industriel en tant qu'opérateur technique de service"e-santé", pour le professionnel de santé et pour l'usager », dans Christian HERVÉ, Michèle STANTON-JEAN et Éric MERTINENT (dir.), Les systèmes informatisés complexes en santé, coll. « Thèmes et commentaires », Paris, Dalloz, 2013, p. 95 et s.

[66] Cf. en particulier la presentation de l'association Medtech Europe (https://www.medtecheurope.org.): « MedTech Europe, from diagnosis to cure – Homepage : "*We represent Diagnostics and Medical Devices manufacturers operating in Europe. There are more than 500,000 products, services and solutions currently made available by the medical technology industry. These range from bandages, blood tests and hearing aids to cancer screening tests, pacemakers and glucose monitors.*". Il s'agit, d'abord, des fournisseurs des éléments du système, qui permettent la collecte, le stockage, le traitement et l'accès aux données médicales : les éditeurs de logiciels utilisés par le monde médical, les producteurs, fournisseurs d'implants médicaux, de prothèses, de robots ou d'objets connectés, les opérateurs de services de stockage y compris de *cloud*.

[67] Sur ces 'nouveaux métiers', lire l'article de J. HERVEG et J.M. van GYSEGHEM, « Un nouveau métier de la santé : la sous-traitance des données du patient. », in *Droits, Normes et Libertés dans le cybermonde*, Liber Amicorum Yves POULLET, Cahier du CRIDS, Larcier, n° 43, p. 747 et s.

[68] « *L'Etat choisit Microsoft pour les données de santé et crée la polémique. Le gouvernement français a pris la décision d'héberger les informations de santé de millions de français …La polémique ne pouvait pas éclater à un pire moment. Quelques jours avant de lancer avec l'Allemagne le projet d'informatique en ligne européenne Gaia-X pour la protection des données dans le « cloud computing », le gouvernement français doit défendre sa décision d'héberger les informations de santé de millions de Français sur les serveurs de l'américain Microsoft…* » (Les échos, 4 juin 2020, article disponible sur le site des échos à l'adresse suivante : https://www.lesechos.fr/tech-medias/hightech/letat-choisit-microsoft- pour-les-donnees-de-sante-et-cree-la-polemique-1208376). Cette décision gouvernementale française justifiée par l'absence de prestataires européens présentant les qualités requises a été largement critiquée. « *Comment soutenir ce choix alors que le Président de l'Agence Nationale de Sécurité des Systèmes d'Information s'oppose publiquement aux géants du numérique qui représenteraient une attaque pour nos systèmes de "santé mutualiste" ?*
Comment soutenir ce choix alors que la CNIL mentionne dans le contrat liant le "Health Data Hub"

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

souvent à la demande des professionnels de santé mais également qui, grâce à des outils technologiques et en particulier de l'IA, peuvent se substituer à eux.

En effet, aux fonctions d'aide aux professionnels de santé assumées par les acteurs technologiques, ces derniers peuvent par leurs services rendus directement aux patients-consommateurs, se substituer aux professionnels de santé. On s'inquiète du rôle toujours plus grand joué par des entreprises dont les services remplacent l'intervention des praticiens de l'art de guérir ou plus largement des professionnels de santé. On assiste ainsi à un phénomène d'ubérisation de la médecine[69] ou selon la formule de MENECEUR[70] de « tentative de confiscation de la médecine par l'industrie numérique ». Déjà en 2009, le CNOM[71] *« s'inquiète du fait que les prestations proposées directement via des plateformes par les assureurs complémentaires ou les mutuelles en santé installent de fait une rupture concurrentielle dans l'organisation territoriale des soins et le parcours de soins. En outre, ces plateformes qui indiquent être accessibles 7j/7 et 24h/24 soulèvent la question de leur cohérence avec les Centres 15 ou interconnectés.* ». On sait que des sociétés proposent contre rémunération des analyses de vos données génétiques, certes apparemment pour vous aider à mieux connaître vos ascendants ethniques ou raciaux, parfois au-delà, pour vous conseiller médicalement, parfois enfin pour revendre à prix d'or leurs analyses ou les simples données à des tiers intéressés[72], qu'il s'agisse de potentiels employeurs, sociétés d'assurance ou organismes de crédit[73]. Incontestablement ces services tombent sous l'application de la directive sur le commerce électronique du 8 juin 2000[74]. Mais au-delà des prescrits de la Directive bien insuffisants pour protéger les patients, il apparaît évident que des exigences supplémentaires s'imposent afin de responsabiliser les différents acteurs et de protéger la santé publique et privée. Il peut s'agir de définir des critères de qualité professionnelle des prestataires de soins, leur mode d'authentification et leur formation, d'imposer, comme préalable à leur intervention, la nécessité d'une demande d'un praticien de l'art de guérir et, par la suite, de l'information à ce dernier des résultats de l'analyse et surtout d'exiger des mesures strictes de sécurité et de confidentialité de même qu'une information claire et précise du patient tant sur le recours par eux aux technologies de l'intelligence artificielle qu'à propos des limites de ces dernières[75]. C'est en ce sens que l'activité de télémédecine a été fortement réglementée

à Microsoft "l'existence de transferts de données en dehors de l'Union européenne dans le cadre du fonctionnement courant de la plateforme »

[69]Comme le note RIGBY en introduction du n° spécial de l'AMA Journal of Ethics dédié aux « *Ethical Dimensions of using AI in Healthcare* » : « *An artificially intelligent computer program can now diagnose skin cancer more accurately than a board-certified dermatologist.ù34ù Better yet, the program can do it faster and more efficiently, requiring a training data set rather than a decade of expensive and labor-intensive medical education. While it might appear that it is only a matter of time before physicians are rendered obsolete by this type of technology…"*

[70]Y. MENECEUR, *L'intelligence artificielle en procès,* Bruylant, Bruxelles, 2020, p. 126 et s.

[71]CNOM, *La Télémédecine face au risque d'ubérisation des prestations médicales : Rappel des positions du Conseil national de l'Ordre des médecins*, Session du 8 février 2018).

[72]La thèse de G. VERHENMEN (*op. cit.,* p. 42) décrit ainsi le cas des labos DANTE.

[73]Y. POULLET, « Quelques réflexions d'un juriste à propos des données génétiques et …d'un rapport récent de la Fondation Roi Baudouin, in *RDTI, 2018, n° 73, p. 19 et s.,* en particulier le n° 10_._

[74]Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique, *J.O.C.E.*, L 178 du 17 juillet 2000, p. 1 et s. Il s'agit en effet de « *services prestés normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services* ».

[75]Dans le même sens, l'avis émis par la CNOM : « *L'ordre des médecins affirme donc de nouveau qu'à ses yeux, la sécurité des prises en charge impose de réglementer les offres des plateformes privées et*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

en France par le décret du 19 octobre 2010 relatif à la télémédecine[76], soumise à nombre de conditions en particulier pour son financement et s'insère nécessairement dans le programme national tel qu'il est relayé en fonction des besoins locaux par les Agences régionales de santé. Enfin, on note que l'utilisation de l'IA permet à des sociétés externes au monde de la santé, en particulier les plateformes, d'utiliser des données obtenues dans le cadre de leurs activités à des fins médicales, c'est-à-dire de déduire de données d'utilisation de leurs services des données sur la santé de leurs clients[77]. Ainsi, un directeur de recherches de MICROSOFT Europe, B. SCHRODER, écrit[78] : « *Nous sommes maintenant capables, de résoudre de toutes nouvelles classes de problèmes, telles que la reconnaissance d'image ou la transcription de la voix. Nous pouvons prédire des événements non modélisables. Par exemple, Cornell University détecte la survenance de l'état dépressif de patients bipolaires en analysant les changements dans la frappe de messages sur l'écran d'un smartphone. Un algorithme de Microsoft prévoit un diagnostic futur de cancer du pancréas ou de poumon par l'analyse de l'historique des mots clés entrés dans un moteur de recherche.* ». GOOGLE a investi massivement dans le domaine de la santé. Ainsi, la société VERIFY entend « *rendre utiles les données mondiales sur la santé afin que les gens puissent jouir d'une vie plus saine* », on cite également les filiales Deep Mind Health (en matière de neurobiologie) ou CALICO (en matière de lutte contre le vieillissement). Les mêmes stratégies sont développées par APPLE, FACEBOOK[79], IBM (Watson) ou AMAZON. Enfin, on souligne l'utilisation de plus en plus grande par des sociétés des données de fonctionnement du cerveau pour des applications de marketing[80].

---

que les activités médicales qu'elles proposent soient soumises aux mêmes obligations réglementaires et déontologiques que les autres formes de pratiques médicales dans un parcours de soin. Au nombre des obligations doivent figurer : l'information de l'usager et son consentement exprès ; – la confidentialité des données de santé recueillies et leur non exploitation à d'autres fins, que celles pourquoi elles ont été collectées ; – l'inscription de la conclusion de l'acte dans le dossier du patient ; – la continuité des soins entrepris ; l'information des médecins habituels du patient, et en particulier son médecin traitant, ou constituent sauf opposition formalisée de la part du patient ; – l'absence de publicité de nature commerciale ; – le non détournement de patientèle ; – l'absence de rémunération « à la minute ». (CNOM, *La Télémédecine face au risque d'ubérisation des prestations médicales : Rappel des positions du Conseil national de l'Ordre des médecins*, Session du 8 février 2018).

[76] Ce décret est pris en application de l'article L 6316-1 du code de la santé publique issu de la loi du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires (HPST) qui précise dans son dernier alinéa : *« La définition des actes de télémédecine ainsi que leurs conditions de mise en œuvre et de prise en charge financière sont fixées par décret, en tenant compte des déficiences de l'offre de soins dues à l'insularité et l'enclavement géographique. »*

[77] Sur ce mouvement et les nombreux exemples, lire le remarquable ouvrage de Y. MENECEUR, *L'intelligence artificielle en procès,* Bruylant, Bruxelles, 2020, p. 113 à 140.

[78] B. SCHRODER, *Vie Privée, transparence et démocratie,* Actes du Colloque du REHNAM, Namur le 28 novembre 2019, Y. Poullet (éd.), Cahier du CRIDS, n° 50, Larcier, 2020.

[79] Facebook a notamment développé un logiciel IA qui surveille le comportement des utilisateurs de son réseau social pour prévenir les dépressions et les suicides

[80] "_The possibility of non-invasively identifying such mental correlates of brain functional differences is of particular interest for marketing purposes. Over a decade ago, McClure *et al.* (2004) used fMRI to show functional differences (increased activation in the dorsolateral prefrontal cortex, hippocampus and midbrain) in the brain of people knowingly drinking Coca Cola as opposed to the same people drinking unlabeled Coke. Their results showed that marketing strategies (e.g. the Coca Cola label) can determine different responses in the brain of consumers (McClure *et al.* 2004). These results have pioneered the establishment of a spin-out branch of neuroscience at the intersection with marketing research called neuromarketing, which has expanded rapidly over the past decade. Today, several multinational companies including Google, Disney, CBS, and Frito-Lay use neuromarketing research services to measure consumer preferences." (_M. IENCA et R. ADORNO, Towards new human rights in the age of neuroscience and neurotechnology, *Life Sciences, Society and Policy,* 2017, 13 ;5, p. 4 et s.). Voir également l'ouvrage du Dr E. TOPOL, *Deep medecine. How Artificial intelligence can make Healthcare Human Agency Again*, Basic Books, 2019

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

15. Du partage des données : où est le secret professionnel ? – La Commission encourage le partage des données au niveau sectoriel (et donc au niveau des acteurs de la santé) comme intersectoriel[81], non seulement en envisageant de mettre sur pied des accords type, pour régler en particulier les questions de propriété intellectuelle, de protection des données, de concurrence et de responsabilité. L'effectivité du règlement proposé par la Commission appelé '*Data Governance Act*'[82] reposera sur la création d'un nouveau métier d'intermédiation, contrôlé par des instances nationales : les services de partage des données qui peuvent et, sans doute dans le cadre des données médicales, doivent être d'abord sectoriels. Ces prestataires de services de partage de données devront jouer un rôle clé dans l'économie fondée sur les données. Ils facilitent l'agrégation et l'échange de quantités substantielles de données pertinentes[83]. Ces « intermédiaires de données » proposeront en effet des services mettant en relation les différents acteurs – les uns, fournisseurs de données, les autres, preneurs de celles-ci – et contribueront à la mise en commun efficace des données ainsi qu'à la facilitation de leur partage. En ce qui concerne le partage des données à caractère personnel en particulier, ils seront chargés de veiller au respect des dispositions du Règlement général de protection des données et assisteront, le cas échéant, les personnes concernées dans l'exercice de leurs droits. Ces intermédiaires de données seront indépendants et neutres, à la fois par rapport aux détenteurs de données et aux utilisateurs de ces données, et leur statut facilitera, on peut l'espérer, l'« *émergence de nouveaux écosystèmes fondés sur les données qui soient indépendants de tout acteur jouissant d'une puissance significative sur le marché* ». Dernière initiative attendue : alors que l'utilisation du *cloud* par nos entreprises reste à la traîne, le lancement d'un cloud européen, garantissant aux utilisateurs la non surveillance de masse par les autorités policières ou de renseignement, est à noter[84].

On ajoute que la proposition permet également à des personnes privées, en spécifiant les finalités de ce transfert (ex : aide à une politique de santé, de l'environnement, de la mobilité, etc.), de mettre à disposition des administrations leurs données. La Commission qualifie d'« altruiste », ce transfert de leurs données par des particuliers. Afin de sécuriser ces transferts (ne serait-ce que pour assurer la protection des données à

[81] *"Sharing and use of privately-held data by other companies (business-to-business – B2B – data-sharing). In spite of the economic potential, data sharing between companies has not taken off at sufficient scale. This is due to a lack of economic incentives (including the fear of losing a competitive edge), lack of trust between economic operators that the data will be used in line with contractual agreements, imbalances in negotiating power, the fear of misappropriation of the data by third parties, and a lack of legal clarity on who can do what with the data (for example for co-created data, in particular IoT data)."* COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data, COM/2020/66 final

[82] Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la gouvernance européenne des données (acte sur la gouvernance des données), Bruxelles, le 25.11.2020, COM(2020) 767 final 2020/0340(COD)

[83] Ces intermédiaires peuvent ainsi veiller à adapter les données, les enrichir, les convertir à un format standard et interopérable, etc.

[84] Voir à ce sujet, les réflexions de la Commission sur le besoin d'une réponse au CLOUD Act américain, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data, COM/2020/66 final. Le « *Clarifying Lawful Overseas Use of Data Act* », ou Cloud Act, a été adopté par le Congrès américain le 23 mars 2018. Cette loi autorise, à certaines conditions, le gouvernement américain et ses services spécialisés à accéder à des données à caractère personnel stockées à l'étranger.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

caractère personnel !), la Commission prévoit l'intervention d'organisations également qualifiées d'altruistes[85], que nous décrirons au paragraphe suivant. L'objectif de ces dispositions reconnaissant l'altruisme des données : « *Data for Public Good* » est clairement de permettre au secteur public de disposer de données en nombre suffisant pour lancer des initiatives d'utilisation de l'IA au bénéfice de l'intérêt général[86].

Multipliée dans le contexte du développement des systèmes d'intelligence artificielle, l'intervention de non professionnels de santé à l'appui, voire en substitution, de professionnels de santé soulève la question délicate de l'application à ces intervenants des obligations de secret professionnel. Les dialogues autrefois singuliers qui les fondent et que le droit entend protéger s'évanouissent au gré des réseaux qu'ils empruntent, des bases de données dans lesquels les données collectées s'engouffrent, les systèmes qui traitent ces dernières et les « *clouds* » où elles attendent de nouvelles utilisations. Soyons clairs : les technologies de l'information et de la communication multiplient les flux et transforment le dialogue à deux en un dialogue à voix multiples au sein de réseaux toujours plus larges, censés apporter un plus dans la qualité des soins ou des conseils à la personne à l'origine du secret. Le secret s'évente, se partage au sein de ces réseaux, se dépose ; il s'étend à des sous-traitants, à des sociétés ou des métiers nouveaux créés en dehors du cercle désigné par nos lois sur le secret professionnel. Secret partagé mais également secret déposé : les avantages d'une technologie qui permet l'accès sécurisé à tout moment tout en le restreignant, ajoutera-t-on aux seules personnes autorisées, suggèrent aux patients de déposer leur secret… dans l'attente de la lecture par autrui. Le dialogue n'est plus à l'origine du secret, il suivra peut-être. La volonté de favoriser l'effectivité du service au client justifie la création de vastes répertoires où sont identifiées *a priori* les relations entre les clients et leurs « confesseurs ». On pense à l'efflorescence des dossiers « santé » déposés sur des serveurs privés ou publics dans le cadre de réseaux télématiques de santé. Les ordres professionnels eux-mêmes, les autorités publiques encouragent les initiatives de partage et favorisent ces échanges au nom tantôt de la diminution des coûts, tantôt de la qualité et de la continuité des soins, tantôt des nécessités de la recherche, sans doute au risque de voir les données protégées par ce secret désormais déposé ou partagé au gré des réseaux multiples ou déposé, devenir objet de vente, comme l'a montré la révélation d'une cession par des hôpitaux de données relatives à leur patient[87].

[85] Les « organisations altruistes en matière de données reconnues dans l'Union » devraient, selon des exigences dont le respect sera vérifié par l'autorité nationale *ad hoc,* être en mesure de collecter des données pertinentes directement auprès de personnes physiques et morales ou de traiter les données collectées par d'autres et ce moyennant le consentement des personnes concernées. Par organisation altruiste, on entend des entités publiques ou privées servant des fins d'intérêt général « *comme les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, l'établissement plus aisé de statistiques officielles ou l'amélioration de la prestation de services publics. Le soutien à la recherche scientifique, et notamment au développement technologique et à la démonstration, à la recherche fondamentale, à la recherche appliquée et à la recherche financée par des fonds privés, devrait également être considéré comme une finalité d'intérêt général.* ».

[86] « *Le présent règlement vise à contribuer à l'émergence de réserves de données mises à disposition selon le principe de l'altruisme en matière de données, qui soient d'une taille suffisante pour permettre l'analyse des données et l'apprentissage automatique,* » (Exposé des motifs, n° 35)

[87] Voir en particulier la cession de données médicales par le National Health Institute anglais à la société Deep Mind de Google. À propos de ce dernier événement que les journaux ont relayé avec indignation, la contradiction du comportement des hôpitaux avec les exigences de la loi Vie privée ou Protection des données a été soulignée dans la mesure où cette loi limite considérablement la circulation des données en particulier médicales (voir *infra,* n°). L'infraction au secret professionnel a été peu mentionnée. D'où la question : la loi Vie privée ne suffit-elle pas à protéger l'intérêt de la personne concernée, en l'occurrence,

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

16. Les questions croissantes de dignité et de justice sociale – L'attention à l'impact d'une société numérique sur les groupes vulnérables constitue une préoccupation essentielle relevée par nombre d'instances internationales dont l'Europe, au premier chef. On songe à la multiplication des protections légales nouvelles accordées, dans l'environnement numérique, à l'enfant, à la femme, au consommateur, au travailleur, aux minorités culturelles, ethniques et religieuses, aux dits LGBT. Les systèmes d'intelligence artificielle et les robots donnent à l'humanité d'aujourd'hui une assistance peu commune à l'action, à la perception et à la cognition. En ce sens, ils représentent un moyen extraordinaire de lutte contre les vulnérabilités. Quelques exemples parmi d'innombrables : les exosquelettes permettent aux personnes de retrouver un membre perdu ; grâce à certains implants, des aveugles peuvent recouvrer partiellement du moins les sensations de la 'vue'[88]

Cette facette positive des technologies du numérique ne peut cependant cacher une autre réalité : celle de voir nos vulnérabilités accrues du fait du numérique. Les fractures numériques rejoignent les fractures économiques et, s'y on n'y prend garde, les renforceront. A cet égard, on s'inquiète du non accès de certaines couches de populations à certains produits ou services d'intelligence artificielle pourtant nécessaires à leur santé et à leur épanouissement. Ainsi, quel patient pourra avoir accès aux *body implants* capable de réguler leur tension artérielle, d'éviter l'hyper- ou l'hypoglycémie, lorsqu'on sait le prix de tels dispositifs ? Seuls les riches aveugles pourront-ils bénéficier des bénéfices de l'implantation de rétines artificielles, des installations domotiques et aide soignants qui leur garantiront la sécurité à domicile ? Enfin, ne risque-t-on pas avec les technologies de l'homme augmenté de voir une société duale des maîtres et des esclaves ? L'irruption du numérique dans la santé permet nous l'avons vu (_supr_a, n° 12) d'augmenter les capacités de l'homme *via* des implants corporels permettant par exemple de décupler la mémoire, de les relier à des intelligences artificielles présents dans des ordinateurs externes ou de lutter contre la vieillesse ou par des mani-

le patient et ne doit-on pas dès lors rejeter comme un fruit du passé la protection du secret professionnel ? Si, indéniablement, la loi Vie privée s'applique aux détenteurs de secrets professionnels, responsables de traitement et que l'obligation, en particulier de sécurité des traitements, reçoit du fait du secret une interprétation rigoureuse, il n'empêche que notre conviction est inverse : le secret professionnel apporte une protection complémentaire à celle offerte par les lois de protection des données. Les lois de protection des données entendent protéger une partie ; le secret professionnel, une relation. Les lois de protection des données soumettent dès lors à la sagacité de la personne concernée, à son consentement, l'utilisation et la transmission de ses données à caractère personnel y compris médicales. À l'inverse, le secret professionnel subordonne la transmission du secret que constitue le fruit du dialogue entre le professionnel et son « client » à une délibération commune, exceptionnellement à un devoir du professionnel de répondre à un intérêt public. Bref, l'application des seules lois de protection des données, à l'exclusion des protections légales accordées au secret, conduit à introduire une « appropriation » du secret par la personne concernée et, donc, pour ce dernier à la possibilité de disposer gratuitement ou contre rémunération du secret vis-à-vis d'autrui, à la limite qu'il s'agisse de son assureur ou de son employeur. À l'inverse, en matière de secret professionnel, le consentement de la personne protégée ne suffit pas à délier le professionnel de son devoir de maintenir le secret : il appartient à ce dernier de s'interroger sur les raisons et la finalité de la demande de son « client » et, le cas échéant, de refuser la transmission des informations couvertes par le secret professionnel.

[88] « Mais qui ne souhaite pas, grâce à la thérapie génique et les ciseaux à ADN, guérir un petit garçon de 7 ans atteint d'une maladie génétique de la peau ? Qui refuserait aux travailleurs frappés d'incapacité motrice de bénéficier d'exosquelette afin de réintégrer le marché du travail ? "*L'aveugle qui voit, l'hémiplégique qui retrouve l'usage de son bras… La figure de la personne handicapée joue un rôle central, elle suscite la sympathie*", pointe Christian Godin. Et qui, sans problèmes de santé, ne voudrait pas bénéficier également de ces prouesses scientifiques pour accroître son confort de vie ? Qui n'aimerait pas, par exemple, retrouver le sommeil grâce à un pyjama supposément intelligent ou des objets connectés ? » in "L'homme se robotise et le robot s'humanise" (article du 27 janvier 2018, disponible à l'adresse https//www.lesnumeriques.com/vie-du-net/transhumanisme-comment-l-individu-augmente-se-niche-dans-nos-têtes.).

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

pulations génétiques. Si on n'y prend garde, ces possibilités nouvelles de soins ouvrent à terme la voie à une humanité à deux vitesses par définition discriminante si l'offre de telles possibilités reste réservée à ceux qui financièrement peuvent se les « offrir ».

Dès 2005, le Groupe Européen d'éthique des Sciences et des Nouvelles Technologies auprès de la Commission européenne[89] affichait sa préoccupation à propos du caractère discriminatoire de l'utilisation de ces implants. En particulier, les questions de dignité humaine et surtout de non-discrimination dans l'accès aux soins[90] étaient épinglées. Ainsi, le Groupe s'interrogeait sur les possibilités *via* de tels systèmes de manipuler l'humain et d'attenter ainsi à sa dignité, en le mettant au service d'un objectif non de développement personnel mais de finalité purement économique. Par ailleurs, le fait que ces technologies ne fassent pour le moment l'objet d'aucun financement par la sécurité sociale même lorsqu'ils apparaissent nécessaires dans le cas d'un traitement médical (voir l'exemple du régulateur d'insuline en cas de diabète) et *a fortiori* lorsqu'ils peuvent à juste titre être considérés comme des dispositifs de « bien-être » rendent leur accès difficile à certaines couches de population. La réflexion du Groupe d'éthique trouve à s'appliquer bien plus encore lorsqu'on s'interroge de manière plus globale sur les technologies visant à augmenter l'homme, déjà présentes sur le marché ou futuribles, objets des fantasmes du « transhumanisme »[91]. En d'autres termes, ne faut-il pas comme le préconisait l'avis cité, lancer un vaste débat public de « *Technology Assessment* » sur les balises à proposer, voire imposer, à de tels développements. Enfin, le Groupe s'inquiétait des droits de propriété intellectuelle entourant de telles innovations qui risquaient de priver nombre d'acteurs de la possibilité d'avoir accès à de tels progrès. Le financement par la sécurité sociale de l'accès à certaines innovations en matière de santé est sans doute une solution à explorer.

La dissymétrie informationnelle et la non transparence du fonctionnement de nos systèmes d'information et, en particulier d'intelligence artificielle, expliquent notre vulnérabilité. S'ajoute le fait que des systèmes d'intelligence artificielle décuplent la puissance de ceux qui les opèrent, en particulier dans le domaine de la santé. Comme nous l'avons vu, ils autorisent le repérage du profil de santé de chacun et créent la possibilité de prédictions liées à ce profilage comme nous l'avons montré (supra, n° 11). L'utilisation de tels systèmes, si on n'y prend garde, autorise sans doute un meilleur traitement mais, dans le même temps, ouvre la possibilité de toutes les dérives induites par la stigmatisation de certains profils par des acteurs du secteur médical mais plus sûrement par des acteurs externes au secteur : assureurs, employeurs dont l'accès à ces profils peut devenir aisé lorsqu'on pense par exemple à la collecte facile et in-

[89] Avis n° 20 du 16 mars 2005, « Aspects éthiques des implants TIC dans le corps humain », avis remis sur base du rapport de son président Stefano RODOTA.

[90] Sur ce thème, l'article de F. DREIFUSS-NETTER, « L'inégalité dans l'accès aux soins », *ANAP*, n° 17, 2011, p. 20 et s.

[91] « *Le transhumanisme est un mouvement philosophique et culturel soucieux de promouvoir des modalités responsables d'utilisation des technologies en vue d'améliorer les capacités humaines et d'accroître l'étendue de l'épanouissement humain* » G. HOTTOIS, *'Le transhumanisme est-il un humanisme ?' Académie royale de Belgique, Bebooks*, 2015, 32. A la différence du transhumanisme, le posthumanisme envisage le remplacement de l'humain par des entités artificielles non humaines qui succéderaient à l'être humain. Il s'agirait de robots doués d'intelligence (artificielle), capables d'émotions, d'empathie et de décisions, susceptibles d'évoluer et de se reproduire (sur cette vision du futur, lire W. WALLACH et C. ALLEN, *Moral Machines, Teaching Robots Right from Wrong*, Oxford University Press, 2009. Sur les mouvements transhumanistes et posthumanistes, lire Le transhumanisme : une anthologie (sous la direction de F.DAMOUR, S. DEPREZ et A. ROMELE), L' Harmattan, 2020.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

suffisamment réglementée des données génétiques. Ces profils de santé sont construits de manière non transparente par les systèmes d'intelligence artificielle et sur base de nombreuses catégories de données et selon des poids qui peuvent évoluer au fur et à mesure de la rencontre du système avec de nouvelles données. Ce constat amène à la nécessité d'un réexamen de la notion de discrimination et de son application. Les discriminations dans le cadre des décisions traditionnelles se fondaient souvent sur des critères uniques et souvent évidents : la race, la religion, les opinions politiques ou philosophiques, l'appartenance syndicale, liste de critères qui correspondent aux données qualifiées de sensibles par les législations de protection des données. Cette approche des risques de discrimination par la nature des données nous apparaît bien partielle à l'heure des systèmes d'intelligence artificielle où les risques de discrimination reposent désormais sur la méthode utilisée par le traitement et non sur la nature des données : ainsi, dans le cadre du recrutement d'employés dans une multinationale, un système d'intelligence artificielle peut, parfois suite à des biais inconscients ou non, exclure des personnes habitant telle sous-région, ayant telle qualification ou telle composition familiale ou telle hérédité, critères indiquant un risque sanitaire plus ou moins élevé. Outre qu'il est dès lors difficile pour ces personnes de se grouper et d'agir, on relève que la discrimination opère désormais suivant des critères plus nombreux et apparemment plus neutres, dont c'est la seule conjugaison qui les rend discriminants. Ces potentialités des applications du numérique ne visent plus un groupe d'individus bien déterminé comme le sont les catégories nommées traditionnellement et dont le statut est souvent protégé tant par la loi et par les associations qui défendent la cause de ces catégories, mais des personnes répondant à un même profil. Ces personnes sont soumises dès lors à des décisions ou des jugements fondés sur ce profilage. Comme l'écrit très justement NAUDTS (2019) à la suite d'autres auteurs, "*Groups are no longer defined as a conglomerate of individuals bound or formed by explicit ties, such as salient traits (Vedder, 1999 and 2000 ; Taylor, Floridi & Van Der Sloot, 2017). Moreover, the purposes for which, or the contexts within which, algorithms can be deployed are extremely varied. Therefore, the current scope of non-discrimination legislation seems too narrow to effectively counter the possible negative and unfair effects of algorithmic differentiation.* »

3 Un cadre juridique en voie d'élaboration

17. De la triple nature juridique des systèmes d'intelligence artificielle en matière de santé – Le droit opère toujours à travers des qualifications juridiques par lesquelles il saisit la réalité. Ces qualifications ne sont pas de toute éternité, elles constituent des réponses aux exigences d'une réalité sociale, économique ou technologique, que la loi crée, que la jurisprudence interprète au regard de circonstances concrètes et que la doctrine analyse sans cesse. En l'occurrence, comment qualifier les applications d'intelligence artificielle que nous venons de décrire et quelles règles le droit applique-t-il sur base de telles qualifications ? Il est clair que ce régime juridique ne peut s'entendre que d'une combinaison de nombre de qualifications juridiques et ce en fonction de l'angle juridique sous lequel on aborde l'application en question. Par exemple, sous l'angle de la propriété intellectuelle, le système d'intelligence artificielle pourra être qualifié d'œuvre protégeable par le droit d'auteur ou d'invention susceptible de

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

brevets ; la question de la création par certains systèmes d'intelligence artificielle de produits dérivés ou de solutions originales pose la question de savoir si le système, la machine, peut être qualifié d'auteur, etc. ; dans le domaine de la responsabilité, peut-on considérer le système IA comme un produit et lui appliquer le régime de responsabilité sans faute de la directive sur la responsabilité du fait des produits de 1985 ? Ces questions mériteraient un développement que les limites de l'article ne permettent pas. Nous nous en tiendrons à trois qualifications majeures. Un système IA utilisé dans le domaine de la santé dans la plupart des cas, constituera, à la fois, un traitement de données à caractère personnel soumis dès lors au RGPD, à la fois, un dispositif médical au sens du règlement de 2017 sur les dispositifs médicaux et, demain, également, un système d'Intelligence artificielle si on se base sur la proposition de règlement dit *AI Act* du 21 avril 2021, actuellement en cours de discussion dans le cadre du trilogue : Commission, Conseil et Parlement.

Cette combinaison de qualifications et donc de régimes, n'est pas sans soulever quelques difficultés. Comment organiser leur coexistence et la cohérence de leurs mises en application ? Nous chercherons à répondre à cette question loin d'être évidente. Notons d'emblée que les dispositions législatives européennes auxquelles nous nous sommes référés, approchent la même réalité sous des angles d'approche différents ou pour être plus précis, en fonction de risques de nature différente. Les risques couverts : de la protection des données à caractère personnel (liberté individuelle), aux risques de santé et de sécurité épinglés par le règlement sur les dispositifs médicaux et, au-delà, s'élargit également aux risques collectifs, voire sociétaires, dans la proposition réglementaire. Il est coutume d'affirmer que notre autonomie trouve sa consécration en droit dans les multiples prescrits du RGPD. L'affirmation n'est pas fausse. Elle invite cependant à souligner quelques lacunes que présente l'application du RGPD lorsqu'il s'agit de prendre en compte l'ensemble des risques liés aux applications de l'IA. Notre propos introductif au chapitre laissait entendre que si l'autonomie est une valeur éthique essentielle lorsqu'on analyse les enjeux des applications fondées sur les réseaux neuronaux, d'autres valeurs éthiques doivent compléter notre réflexion. Ce qui caractérise les enjeux de l'IA en particulier dans ses applications de santé, c'est qu'ils débordent de loin les aspects de protection d'intérêts et de libertés individuels, ceux pour la protection desquels ont été adoptées les législations de protection des données. Les enjeux environnementaux, de justice sociale, de démocratie sont désormais au cœur des textes éthiques qui se succèdent dans les instances internationales. L'IA certes peut être un moyen de prévention et de lutte contre ces risques collectifs et sociétaires, elle est également cause de leur aggravation. Les applications IA soulèvent des problématiques éthiques bien au-delà de la seule protection des données. Elles représentent un défi pour la justice sociale, réservant certains avantages aux seules personnes capables d'acquérir les outils IA et pour la démocratie, dans la mesure où elles normalisent parfois à l'excès les comportements et favorisent la manipulation des masses. La protection des consommateurs, des SME et l'étiquetage collectif de personnes constituent d'autres facettes de la réflexion. A ce propos, on citera le paragraphe 25 du projet de recommandation de l'UNESCO sur l'éthique de l'I.A. : "*It should be recognized that AI technologies do not necessarily, per se, ensure human and environmental and ecosystem flourishing. Furthermore, none of the*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

processes related to the AI system life cycle shall exceed what is necessary to achieve legitimate aims or objectives and should be appropriate to the context. In the event of possible occurrence of any harm to human beings, human rights and fundamental freedoms, communities and society at large or the environment and ecosystems (nous soulignons)*, the implementation of procedures for risk assessment and the adoption of measures in order to preclude the occurrence of such harm should be ensured*".

Enfin, on note que le développement des systèmes d'IA est de plus en plus le fait des *Tech Giants* (ou GAFAM) et des plateformes et pose des questions au regard du droit de la concurrence et du rôle de l'Etat. Ces questions doivent être abordées de manière concertée entre les autorités en charge de ces diverses thématiques. Le respect des libertés et des droits fondamentaux, et notamment du droit à la vie privée et à la dignité humaine, mais aussi à la liberté d'expression et du principe de non-discrimination, mais également des impératifs de justice sociale, de diversité culturelle et de démocratie, doivent être garantis. On ajoute qu'au fur et à mesure des textes, l'approche '*risk-based's'affirme progressivement. Ces risques s'attachent tantôt à un traitement, objet du RGPD, tantôt à un produit mis sur le marché, un dispositif médical fonctionnant grâce à un logiciel dans le règlement de 2017 ou dans la proposition réglementaire en cours de discussion. Enfin, on notera que les acteurs visés par ces différents textes diffèrent. Restreints aux seuls responsables de traitements et sous-traitants dans le cas du RGPD, les deux autres textes prennent en compte les nombreux acteurs qui interviennent dans la chaîne depuis la conception du système, sa mise au point jusqu'à sa commercialisation, son utilisation, la continuité de son fonctionnement jusqu'à sa fin. Notre propos étudie ces trois cadres successivement.*

4 La question de l'application du RGPD – des incertitudes voire des lacunes ![92]

4.1 Le champ d'application du RGPD

18. La question des données dites anonymes et la notion de données de santé –L'analyse des risques posés par les applications d'IA soulève les questions délicates : premièrement, du champ d'application du RGPD et, secondement, de la notion de données médicales. En ce qui concerne le premier point, le RGPD limite sa protection aux seules données à caractère personnel. Certes, cette notion doit s'entendre de manière large puisque au critère d'identifiabilité qui d'une manière ou d'une autre continue à faire référence à la notion d'identité civile et aux éléments de celle-ci, se substitue

[92] Le lecteur trouvera un exposé plus complet sur les questions posées par l'IA à l'application du RGPD, in Y. POULLET, *Le RGPD face aux défis de l'intelligence artificielle,* Cahier du CRIDS, n° 48, 2020

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

progressivement[93] celui d' « individualisation »[94], c'est-à-dire cette possibilité de saisir la personne dans sa singularité, même si l'identité civile ne peut être connue[95].

Notre propos ne s'arrête pas là. Il s'agit de mettre en évidence le fait que la réglementation de l'IA doit également s'appliquer aux données à caractère non personnel, c'est-à-dire les données anonymes prises en compte par le système de *machine learning*. L'argument est double. Premièrement, il note que la puissance de certains systèmes d'IA est telle que des données, pourtant considérées comme rendues anonymes, peuvent être re-personnalisées[96]. En particulier, il a été souligné la possibilité à partir de bases de données anonymisées d'images de fonctionnement du cerveau de retrouver les personnes qui se 'cachent' derrière de telles données[97]. Deuxièmement, on souligne que la plupart des systèmes d'IA, en particulier de profilage, utilisent des données anonymes. Ainsi, dans le cadre d'un profilage permettant de sélectionner les candidats à un logement, l'opérateur d'un système se référera à des données telles que le revenu moyen des personnes originaires de tel quartier, le niveau scolaire des habitants ou leur niveau d'endettement. Limiter les dispositions du RGPD aux seules données à caractère personnel représente dès lors un risque en matière de transparence pour la personne concernée : il est requis d'envisager également les données anonymes qui, dans bien des cas, peuvent également servir à la constitution du profil. Ainsi, conformément aux articles 13, 14 et 15 du RGPD, limiter l'information et l'accès à la personne concernée aux seules données à caractère personnel intervenues dans la fabrication de son profil de candidat à l'emploi et exclure de cette information les données anonymes apparaîtrait comme une information incomplète, voire biaisée. Le récent projet de recommandation du Conseil de l'Europe sur le profilage reconnaît, en ce qui concerne ce type d'opérations, ce besoin d'extension du champ d'applica-

[93] Voir en particulier l'avis du Groupe de l'article 29 sur la notion de données à caractère personnel : « Trois critères ont ainsi été affirmés par le Groupe de travail « article 29 » (dont la fonction de coordination des autorités de protection nationales des données a été transférée par le RGPD à l'European Data Protection Board) : l'individualisation (est-il toujours possible d'isoler un individu ?), la corrélation (est-il toujours possible de relier entre eux les enregistrements relatifs à un individu ?) et l'inférence (peut-on déduire des informations concernant un individu ?). Si le traitement répond à ces trois critères, il sera considéré comme anonyme ; il pourra également l'être s'il ne respecte pas l'un des trois critères, mais seulement après une analyse détaillée des risques de ré-identification (dans son avis du 10 avril 2014 (Avis n° 05/2014 du 10 avril 2014 sur les Techniques d'anonymisation du Groupe de travail « article 29 » sur la protection des données)

[94] Il s'agit de passer, selon le terme heureux de C. de TERWANGNE, de l'identification d'une personne, c'est-à-dire d'une possibilité de retrouver les éléments de son identité légale (nom, prénom, adresse, etc.), à l'individualisation c'est-à-dire la capacité de rapporter à un individu singulier des données, sans que les éléments de son identité légale ne soient connaissables ou connus C. de TERWANGNE, « Définitions clé et champ d'application du RGPD », in DE TERWANGNE C. et ROSIER K. (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR), Analyse approfondie, Cahiers du CRIDS*, n° 44, Bruxelles, Larcier, 2018, p. 64 et s. Ainsi, le tag RFID porté par une personne X se baladant dans un supermarché, ne permettra sans doute pas l'identité de son porteur mais permettra de le localiser au sein de ce supermarché, de tracer, le cas échéant, ses précédents achats voire de connecter de telles informations à celles résultant de ses habitudes de *surfing*.

[95] Sur cette évolution, lire les actes du colloque de Toulouse de 2019 tenu sur l'identité numérique, J. EYNARD (sous la direction de), *L'identité numérique – Quelle définition pour quelle protection ?,* Larcier, Collection Création et communication, Bruxelles, 2020

[96] A cet égard, à propos des données de communications téléphoniques rendues anonymes et la possibilité de les désanonymiser, « On the privacy-conscientious use of mobile phone data », *Scientific Data, No 5*, 11 décembre 2018 (https://www.nature.com/articles/sdata2018286.pdf.).

[97] A cet égard, lire V. RAVINDRA et A. GRAMA, « De-anonymisation Attacks on Neuroimaging Datasets », SIGMOD 21, 20-25 juin, 2021, Virtual event, China, https://doi.org/10.1145/34448016.3457234. : "*In this paper, we present a de-anonymization attack rooted in the innate uniqueness of the structure and function of the human brain. We show that the attack reveals not only the identity of an individual, but also the efficacy with which they performing cognitive tasks.*"

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

tion de la réglementation de protection des données : « *Dans le cadre de l'utilisation croissante de méga données (« big data »), des données à la fois personnelles et non personnelles sont traitées. Par ailleurs, avec des traitements automatisés, basés notamment sur l'utilisation de systèmes d'apprentissage automatique, il est difficile de savoir a priori quelles données permettront des corrélations ou des prédictions relatives à une personne concernée. Dans de tels cas, pour que les données à caractère personnel soient traitées de façon loyale, les organisations devraient garantir la pertinence et la qualité de toutes les données, y compris les données non personnelles, qui pourraient permettre les corrélations ou prédictions relatives à une personne concernée.* »[98].

Le second point souligne qu'il est désormais nécessaire de ne pas limiter la notion de données médicales aux seules données dont le contenu par nature se rapporte à un état de santé. Prenons l'exemple de certaines recherches qui déduisent des mots choisis pour l'interrogation d'un moteur de recherche ou de l'évolution de la frappe sur un clavier d'ordinateur un état de santé de l'internaute. En d'autres termes, la qualification de « sensibles » des données ne tient pas nécessairement à la nature en soi sensible des données traitées mais au résultat de leur traitement, en tenant compte de la finalité de celui-ci, ce que l'EDPB[99] appelle 'les données inférées'. Cette constatation rejoint l'argument en faveur d'une interprétation constructive de l'article 9 du RGPD qui, rattache le caractère sensible non à la nature des données mais au traitement dans lequel ces données sont considérées. Le texte de l'article 9.1.[100] énonce en effet : « *le traitement des données à caractère personnel qui révèle (et non qui révèlent, nous soulignons) l'origine raciale, les opinions politiques, ….* ». Ainsi, c'est le traitement et non la donnée elle-même qui 'révèle' la sensibilité des données. Ce point est essentiel tant de plus en plus c'est à partir de données non sensibles en soi qu'à travers les algorithmes 'intelligents' se déduit un résultat sensible. Enfin, on ajoute l'intérêt de l'ajout par le RGPD parmi les données faisant l'objet d'une protection particulière des données biométriques et génétiques[101], qui sont bien souvent l'objet d'applications en

[98] Voir en ce sens, le point 7.6 de la recommandation récente du Conseil des ministres du conseil de l'Europe en matière de profilage (Recommandation CM/Rec(2021)8 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage, adoptée par le Comité des Ministres le 3 novembre 2021_ :_ "*Dans les cas où les données ont été anonymisées ou pseudonymisées, les responsables du traitement devraient évaluer le risque de réidentification de la personne concernée (en tenant notamment compte des délais, efforts ou ressources nécessaires au regard de la nature des données, du contexte de leur utilisation, des techniques de réindentification disponibles et des coûts correspondants). Les responsables du traitement devraient démontrer l'adéquation des mesures de pseudonymisation ou d'anonymisation des données et garantir leur efficacité. S'il existe un risque de réidentification de la personne concernée, ces données ne peuvent plus être considérées comme anonymisées. Les mesures techniques peuvent être combinées avec des obligations juridiques ou contractuelles afin de prévenir toute possible réidentification de la personne concernée. Les responsables du traitement devraient réévaluer régulièrement le risque de réidentification, eu égard aux avancées technologiques relatives aux techniques de désanonymisation. Les États membres pourraient établir de manière régulière une liste des techniques de pseudonymisation et/ou d'anonymisation à l'usage des responsables du traitement.* »

[99] Voir à ce propos, EDPB, Guidelines 8/2020 on the targeting of social media users, Version 1.0, Adopted on 2 September 2020, en particulier p. 29 et 30.

[100] Le texte de la directive 95/47 se référait non au traitement mais aux données. L'article 8.1 stipulait ; « les Etats-membres interdisent les traitements des données qui révèlent … »

[101] Les données tant génétiques que biométriques présentent des caractéristiques communes : elles s'adressent à une réalité biologique propre à la personne concernée (même si parfois partagée avec d'autres membres de la famille, comme dans le cas des données génétiques) et en tant que telles, elles ne peuvent être modifiées et collent de manière définitive à notre peau. On ne peut s'en affranchir. Sur la nécessité d'une prise en considération des risques particuliers liés aux traitements des données génétiques, lire *Recommandation CM/Rec(2019)2 du Comité des Ministres aux États membres en matière de protection*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

matière de santé de systèmes de *machine learning,* comme les systèmes de prédiction médicale fondés sur les analyses génétiques des personnes concernées[102].

19. La limitation du RGPD aux seuls acteurs : responsable du traitement et sous-traitant – les problèmes liés à la multiplicité des acteurs – Les obligations prescrites par le RGPD sont à la charge de catégories limitées d'acteurs : le responsable du traitement et ses sous-traitants. Le chapitre précédent notait le nombre de personnes impliquées dans la chaîne des acteurs à la fois en amont et en aval du fonctionnement et de l'utilisation d'un système d'IA, sans que ces acteurs soient toujours qualifiables de responsables de traitement ou de sous-traitants. Ainsi, les chercheurs d'un laboratoire de recherche peuvent acquérir sur le marché voire gratuitement des algorithmes d'IA qu'ils appliqueront à leurs recherches en matière de santé ou trouveront sur le Net, des jeux de données par exemple en matière de dessins d'enfants qui serviront de base à des prédictions sur le développement mental d'autres enfants. Pour ces fournisseurs d'éléments nécessaires au fonctionnement d'un système de profilage et qui les offrent commercialement ou non sur le marché (un algorithme de base, un jeu de données nécessaires au *testing*, une base de données), devraient être requis des engagements quant à la qualité du produit, la description des limites de celui-ci et, le cas échéant, la collaboration avec le responsable dans le cadre de l'évaluation des risques et lors de la phase de tests. Même si les qualifications de responsable ou sous-traitant ne peuvent être retenues, les textes cités plaident en effet pour une obligation à charge d'acteurs, intervenant dans la fourniture d'algorithmes, de bases de données servant de jeux de tests ou de mégadonnées, de collaborer avec le responsable du traitement pour diminuer les risques, en particulier en donnant une information sur la qualité et les limites de l'élément fourni au regard de l'objectif poursuivi par ce dernier à travers l'exploitation du système IA de manière à éviter des biais ou des erreurs. On peut imaginer que cette collaboration pourrait l'obliger à participer à la phase de tests pour détecter les éventuels biais présentés par son produit[103]. Sans négliger l'interprétation large donnée à la notion de responsable conjoint par la jurisprudence de la CJUE[104] , on note que les textes récents sur l'éthique de l'IA, le règlement

des données relatives à la santé, adoptée par le Comité des Ministres le 27 mars 2019, lors de la 1342e réunion des Délégués des Ministres. Comparer avec la définition du RGPD, art. 4.13) : « données génétiques », les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question »

[102]Voir à ce sujet, la législation américaine spécifique relative au traitement de données génétiques, le '*Genetic Act'* déjà citée dont l'application est malheureusement limitée aux seuls organismes de santé et donc n'affecte pas les autres acteurs en particulier du marché commercial qui traitent des données génétiques.

[103]A cet égard, le point 3.12. de la Recommandation récente du Conseil de l'Europe en matière de profilage (Recommandation CM/Rec(2021)8 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage, *adoptée par le Comité des Ministres le 3 novembre 2021* : « *Lorsqu'ils acquièrent des données ou des algorithmes d'un tiers, le responsable du traitement et le cas échéant le sous-traitant devraient obtenir de ce tiers la documentation nécessaire à la vérification de la qualité des données et des algorithmes, et de leur adéquation à la finalité poursuivie par le traitement.* »

[104]La responsabilité conjointe est consacrée par l'article 26 du RGPD : « *Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.* ». Sur l'application par la CJUE de ce texte : lire notamment, CJUE 10 juillet 2018, C-25/17, Témoins de Jéhovah, ECLI :EU :C :2018 :551, 65 et ss. ; CJUE 5 juin 2018, C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI :EU :C :2018 :388, 25 et s. Selon les lignes directrices de l'EDPB (Guidelines 07/2020 on the concepts of data controller and processor in the GDPR,

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

sur les dispositifs médicaux et la proposition de règlement IA, deux textes que nous analyserons ensuite, attachent à ces acteurs des obligations spécifiques.

4.2 Les principes du RGPD

20. Rappel des principes – L'article 5 du RGPD institue divers principes qui protègent directement ou indirectement les personnes concernées, en l'occurrence les patients. La loyauté implique que la création et le fonctionnement des traitements soient transparents pour la personne concernée. La finalité doit être déterminée et l'utilisation à des fins incompatibles est interdite ; les données traitées doivent se limiter, selon le principe de minimisation, aux seules données nécessaires à la réalisation des finalités et leur durée de conservation ne pas déborder la durée nécessaire ; le traitement doit être loyal et enfin, la sécurité des données est à assurer. Nous ne pouvons être exhaustif ici et souhaitons nous limiter à quelques considérations sur la façon dont l'utilisation de l'intelligence artificielle dans le domaine de la santé soulève des difficultés d'application de certains de ces principes.

21. Le principe de finalité – L'affirmation du principe de finalité permet de définir la raison légitime du traitement de données et de circonscrire l'utilisation de données dans des limites connues par la personne concernée. Son affirmation soulève dans son application aux systèmes d'IA de nombreuses difficultés[105]. La première concerne la détermination des finalités qui doit avoir lieu préalablement à la collecte des données. On note le vague et le flou des finalités annoncées : « recherche », « Soins de santé », « suivi médical », autant de finalités génériques dont l'énoncé ne permet pas de fixer les '*reasonable expectations'* de la personne concernée à propos de l'utilisation de leurs données[106]. Ce caractère indéterminé est souvent justifié par le fait que la richesse possible des agrégations permise par les algorithmes au sein des *big data* voire l'évolution de celles-ci en fonction de nouvelles données collectées permettent à l'exploitant du système d'entrevoir de nouvelles applications possibles[107]. On conçoit par ailleurs que la notion de finalités compatibles sera souvent invoquée pour permettre l'élargissement des finalités. Il sera utile de maintenir une interprétation stricte des critères retenus par l'article 6.4 du RGPD qui autorise, moyennant le respect de conditions relativement strictes l'usage à des fins compatibles, sans devoir nécessiter la recherche d'une nouvelle base légale[108]. Dans tous les autres cas, il sera nécessaire de fonder le

v. 2.0, 2021, para. 20 et s.) : "*joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue.*" Il est donc nécessaire de déterminer si les finalités d'une part et les moyens d'autre part, ont été déterminés de manière conjointe.

[105] Sur ce principe et ses difficultés d'application dans le domaine de la santé, lire G. VERHENNEMAN, *op. cit.*,_ p. 266 à 327. On rappelle que le principe de limitation des finalités a fait l'objet d'une opinion du défunt Groupe de l'article 29, *Opinion 3/2013 sur la détermination des finalités*, en date du 2 avril 2013

[106] Même si l'EDPB semble accepter du moins en matière de recherche des finalités comme 'recherche sur le cancer' sans devoir être explicite quant au type de cancer ;

[107] Voir ci-dessus, l'exemple de Microsoft (supra, n°) ou la découverte, dans le cadre de laboratoire de recherches, d'un lien entre des données génomiques et une maladie qui peuvent amener à passer de la recherche à l'exécution de soins ou autre exemple, le passage d'une médecine curative à une médecine méliorative.

[108] « *Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

traitement nouveau sur un des cas de légitimité prévue par l'article 6 (consentement, nécessités du contrat, mission publique, etc.)[109].

Toujours à propos de ce même principe, les risques liés à l'impact dans certains secteurs de certains traitements utilisant l'IA peuvent amener à interdire *a priori* leur utilisation à certaines finalités. On cite les craintes d'utilisation de la reconnaissance faciale et dès lors la réglementation stricte qui s'y applique[110]. La loi belge sur les assurances déjà citée, modifiée le 4 décembre 2020 introduit en son article 4.2, une restriction importante d'utilisation de certaines technologies à des fins de collecte de données et, en son article 5, interdit la segmentation de la clientèle fondée sur l'acceptation de tels outils. On doit s'attendre à une multiplication de telles réglementations spécifiques au vu des risques importants de discrimination que représentent les capacités prédictives et décisionnelles de l'IA. Par ailleurs, le statut de simples sous-traitants des entreprises qui, non seulement, offrent aux praticiens de l'art de guérir les dispositifs aptes à suivre la santé du patient mais, également, récoltent les données nées de l'utilisation de ces services, interdit que sur base de ces données ainsi recueillies, ils puissent développer des recherches nouvelles et, le cas échéant offrir des services nouveaux.

22. Et la minimisation des données ? Les principes de minimisation et de proportionnalité rencontrent également des difficultés d'application dans le cadre des traitements utilisant des systèmes d'IA. L'exemple des robots aide-soignant des robots est plus délicat dans la mesure où il est difficile de connaître *a priori* les données qui seront collectées et dont l'étendue et le type peut varier au gré de l'évolution d'un système fondé sur le *deep learning.* Le fonctionnement du système exige, par ailleurs, l'enregistrement de données concernant les tiers, pas seulement les faits et gestes du personnel soignant mais au-delà des tiers par exemple lors de leurs visites aux patients. Enfin, la mise à disposition dans un hôpital ou à domicile d'un robot pendant la durée d'une

garantir les objectifs visés à l'article 23, paragraphe 1, le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres : a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ; b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ; c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10 ; d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ; e) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation. ». En ce sens, l'Opinion 3/2019 de l'EDPB « *concerning the Questions and answers on the interplay between the Clinical trials Regulation (CTR) and the GDPR »,* adoptée le 23 février 2019.

[109] Prenons deux exemples. Mes données ont été recueillies dans le cadre d'une recherche sur le cancer ; demain, le logiciel mis au point est utilisé pour me proposer des services médicaux préventifs. Il sera nécessaire que la firme qui a mis au point le logiciel me demande à nouveau mon consentement si elle souhaite utiliser mes données dans le cadre de cette nouvelle finalité. Une maison d'accueil de personnes âgées, sur base des données recueillies de manière à diagnostiquer l'apparition de symptômes de la maladie d'Alzeihmer envoie mes données à un laboratoire de recherches. L'étude déjà citée du COCIR (COCIR, *Artificial intelligence in EU medical device legislation,* Sept. 2020, p. 12) donne ainsi de nombreux exemples à propos de dispositifs médicaux. Ainsi, un dispositif utilisant l'intelligence artificielle pour la détection de démence « fronto-temporale » pourrait évoluer pour la détection d'autres cas de démence (par exemple celle liée à la maladie de Creutzfeld-Jakob), il s'agit alors d'une nouvelle finalité.

[110] Ainsi, en France, la reconnaissance faciale pour le compte de l'Etat peut être justifiée par l'intérêt public (*article 6 III de l'Ordonnance de 2018*) mais doit faire l'objet d'un Décret en Conseil d'Etat pris après avis de la CNIL. La proposition de règlement de la Commission dite *AI Act* que nous étudierons par la suite, émet également des réserves à propos de l'utilisation de systèmes de reconnaissance faciale

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

maladie ou d'un suivi de soins exige que l'on s'interroge sur le devenir des données enregistrées au lendemain de cette mise à disposition. Pourra-t-on aisément, comme le réclame le RGPD tant par la création du droit à l'oubli que par le principe de pertinence, effacer du système les données relatives au patient avant une autre mise à disposition ou à les restituer à ce dernier ? Sans doute, l'obligation de '*privacy by design'* obligerait le responsable et son sous-traitant à configurer le robot comme tel mais l'obligation ainsi prescrite s'applique, selon le RGPD, au responsable du traitement et non au concepteur.

23. La mise en œuvre des principes de proportionnalité et de minimisation : Les principes de proportionnalité et de minimisation présupposent que l'on puisse *a priori* déduire de la finalité déterminée de l'application les données nécessaires à son obtention et la durée de leur conservation. Or les systèmes dits de *machine learning* fonctionnent grâce à des corrélations statistiques établies sur base de rapprochements souvent non prévisibles de données et exigent donc que les réservoirs de données brassent très largement[111] et puissent stocker les données sur une longue période, ne serait-ce qu'au cas où elles pourraient s'avérer utiles. Quelle solution trouver ? La pseudonymisation[112] de certaines données prônées dans des lignes directrices du Conseil de l'Europe en matière de mégadonnées n'est pas une solution répondant aux principes évoqués même si elle peut contribuer à la sécurité des données[113]. Le projet de recommandation du Conseil de l'Europe sur le profilage, déjà cité, suggère, en son point 3.2. au nom de ces principes, au moins l'application des limites fixées par les « *legitimate expectations* » des personnes concernées : *« Les données personnelles utilisées dans le cadre du pro-*

[111] Ainsi, l'analyse par des systèmes d'intelligence artificielle de vastes biobanques couplées à des données hypothèse purement fictive, il pourrait apparaître, aux yeux de l'administration fiscale lors de l'utilisation de vastes banques de données, que les dirigeants d'entreprise de plus de 200 employés et moins de 400, disposant d'une voiture rouge immatriculée entre telle et telle année, ayant l'habitude de voyages '*all inclusive'* dans les pays méditerranéens, habitant tel type de quartier dans des villes de plus de 50.000 habitants, avec un enfant et un chien, constituent des fraudeurs potentiels. Cet exemple témoigne du fait qu'il est difficile, *a priori* du moins, de fixer les éléments qui serviront à établir le profil.

[112] On se méfiera même de l'anonymisation dans la mesure où de plus en plus les scientifiques estiment que dans le cadre de *Big Data,* la réidentification de données est souvent possible. Le considérant 26 du RGPD estime : « *Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci.* » Ce considérant laisse la place à des interprétations différentes. Faut-il accepter que l'exigence d'anonymisation puisse se suffire du critère de l'absence de moyens 'raisonnables' de ré-identification dans le chef du responsable du traitement ou d'un tiers au moment de la collecte ou exigera-t-on l'absence de tels moyens y compris dans le futur ? Sur ce point, les réflexions de G. VERHENNEMAN, op. cit., p. 217 et s. et l'opinion du Groupe de travail de l'article 29 du 20 juin 2007 sur le concept de données personnelles (WP.136, p. 15 et 16) qui demande de prendre en compte : « *the available technology at the time of the processing and the technological developments* »

[113] Voilà comment les Lignes directrices (Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679), adoptees le 6 février 2018 par le Groupe de l'article 29, s'expriment à ce propos (p. 11), sans résoudre le problème : "*The business opportunities created by profiling, cheaper storage costs and the ability to process large amounts of information can encourage organisations to collect more personal data than they actually need, in case it proves useful in the future. Controllers must make sure they are complying with the data minimisation principle, as well as the requirements of the purpose limitation and storage limitation principles. Controllers should be able to clearly explain and justify the need to collect and hold personal data, or consider using aggregated, anonymised or (when this provides sufficient protection) pseudonymised data for profiling.*"

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

filage devraient être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles seront traitées. Dans les systèmes de 'machine learning' il est difficile de connaître a priori quelles données permettront des corrélations significatives. Par ailleurs, il est important de limiter le traitement de profilage à des catégories de données dont la personne concernée peut raisonnablement s'attendre (légitimement s'attendre) à ce qu'elles soient prises en considération au vu des finalités du profilage. ». Sans doute cette balise est-elle insuffisante et faudra-t-il, avec les praticiens de l'art de guérir, avec le cas échéant une intervention législative fixant elle-même certaines limites aux données utilisées, répondre à des questions, qui sont loin d'être triviales comme les suivantes : « Jusqu'où, une compagnie d'assurances peut-elle utiliser des données relatives aux personnes assurées dans le cadre de l'offre de services individualisés ? » ; « A quel point, la sécurité des personnes âgées dans une maison de repos exige-t-elle une surveillance à tout instant et en tout endroit des pensionnaires ? ; « Que penser de la collecte, par un laboratoire de recherches sur les 'causes' de la maladie de Parkinson qui affecte un patient, de données socio-économiques relatives à cet individu et à ses géniteurs ? ». Que répondra-t-on au médecin zélé qui au nom du bien du patient multiple les données collectées à son sujet ?

24. La qualité des données : On se contentera de se référer au point 7.8 du projet dc recommandations à propos du profilage du Conseil de l'Europe déjà cité. « *Les responsables du traitement et, le cas échéant, les sous-traitants veillent à évaluer de manière critique la qualité, la nature et la quantité des données utilisées en éliminant les données inutiles et toutes celles qui pourraient biaiser les résultats. En particulier, certains seuils minimaux d'exactitude des résultats doivent être respectés. Ils s'assurent de la robustesse du modèle en cas d'apport de nouvelles données…* ». Le respect de cette double exigence – la qualité des données et l'absence de biais – est essentiel dans le cas d'applications de santé. Il est important que les données qui servent au *testing* et par la suite à enrichir le fonctionnement du système, ne présentent pas d'erreur et soient mises à jour. La procédure de vérification de la qualité des données doit permettre de labelliser la base de données qui alimente l'application. « *Mais, comment s'assurer que la donnée est bien conforme à cette vérité, c'est-à-dire correctement étiquetée ? Selon Éric Topol*[114], c'est le médecin expert qui fait office de golden standard de la labellisation. Ainsi, lorsqu'un médecin expert certifie qu'il y a, dans une image, la présence d'un œdème maculaire, cela vaut pour vrai car personne n'est plus qualifié que le médecin expert. Seulement, la littérature regorge de processus de labellisation aux qualités variées[115]

[114]E. TOPOL, « High-Performance Medicine : The Convergence of Human and Artificial Intelligence ». *Nature Medicine* 25, n° 1 (janvier 2019) : 44-56. https://doi.org/10.1038/s41591-018-0300-7.

[115]Par exemple dans les cas de fracture de hanche, les images sont récupérées avec le diagnostic clinique sans qu'un contrôle supplémentaire soit nécessaire. Cela s'explique parce qu'une personne souffrant d'une fracture, même « silencieuse », finira par allez à l'hôpital et être rapidement diagnostiquée par le radiologue. W. GALE *et al.*, « Detecting hip fractures with radiologist-level performance using deep neural networks », *arXiv :1711.06504 [cs, stat]*, 17 novembre 2017, http://arxiv.org/abs/1711.06504. ; Pour la constitution d'une base de données en vue de la détection d'une imagerie musculosquelettique « normale » ou « anormale », des radiologues, certifiés par le conseil d'administration de l'hôpital (Stanford), procèdent à la labellisation manuelle de chacune des 14.863 études (40561 radiographies).P. RAJAIPURKAR *et al.*, « MURA : Large Dataset for Abnormality Detection in Musculoskeletal Radiographs », *arXiv : 1712.06957 [physics]*, 22 mai 2018, http://arxiv.org/abs/1712.06957.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

Là encore, une régulation appuyée sur l'investissement des médecins est fondamentale[116] *pour établir des normes de qualités encadrant le processus de labellisation. ».*[117]. Cette réflexion implique, d'une part, l'importance de la représentation professionnelle lorsqu'il s'agit de données qui nécessitent l'appréciation d'un professionnel de santé et, d'autre part, la nécessité lorsqu'un système neuronal s'appuie sur des données provenant d'une base de données externe de disposer d'une documentation voire d'une certification de qualité de la part du fournisseur des données. En ce sens, on note que tant les textes du Parlement européen, du Conseil de l'Europe que de l'OCDE[118] insistent sur les obligations des fournisseurs de données et des algorithmes de collaborer à la sécurité du système en particulier par une documentation adéquate attestant de la qualité des données et des mesures prises pour éviter les biais.

25. Le principe de sécurité des données et du système – Les multiples risques attachés au fonctionnement des systèmes d'IA sont connus : mauvaise qualité, non pertinence ou non actualisation des données collectées et traitées par le système ; biais ou erreur dans la programmation, évolution imprévisible et opacité du système, sans omettre les risques d'intrusion et d'atteinte au fonctionnement du système. La sécurité des systèmes est donc un principe majeur au vu des conséquences que l'avènement de ces risques peut entraîner dans le cadre du fonctionnement d'un système d'IA utilisé en matière médicale[119]. Les principes dits éthiques du rapport d'experts de la Commission européenne[120] attachent une attention particulière aux besoins d'une évaluation régulière des mesures de sécurité. Comme le note le point 7.7 de la recommandation du Conseil de l'Europe relatif au profilage : « *Afin d'assurer la confiance dans les systèmes d'IA, les responsables du traitement et, le cas échéant les sous-traitants, veillent à l'utilisation de systèmes fiables et sûrs, notamment en ce qui concerne la mise sur pied de procédures en cas de non-fonctionnement, d'erreurs ou d'incohérences pendant toute la durée de vie du système. Ils s'assurent de manière régulière tout au long de la vie du système que celui-ci est fiable et que ses résultats sont conformes au modèle et sont reproductibles. Le système devrait être robuste pour résister aux attaques ou*

[116] T. JACQUES *et al.*, « Proposals for the Use of Artificial Intelligence in Emergency Radiology ». *Diagnostic and Interventional Imaging*, 2 décembre 2020.

[117] I. DAQUIN, article cité. L'auteur décrit les procédures mises en place à propos de la constitution d'une big data d'images permettant une tomographie en cohérence optique. L'algorithme peut classer les images dans plusieurs catégories : dégénérescence maculaire liée à l'âge (DMLA), une rétinopathie diabétique, drusen ou normal

[118] OCDE, Recommandation du Conseil sur l'intelligence artificielle, OECD/LEGAL/0449, adopté par le Conseil des Ministres de l'OCDE, le 22 mai 2019, disponible à l'adresse : https://legalinstruments.oecd.org/api/print?ids=648\&lang=fr (consultée pour la dernière fois, le 22 janvier 2021).

[119] A cet égard, la révélation en 2018 par des documents internes d'IBM que le supercalculateur WATSON Health aurait émis des recommandations inappropriées pour des patients atteints de cancer (Voir l'article de C. ROSS, « IBM's Watson supercomputer recommended « unsafe and incorrect » cancer treatments, internal documents show », *STAT*, 25 juillet 2018, cité par Y. MENECEUR, *op. cit.*, p. 123)

[120] Comme le note la recommandation n° 5 de l'OCDE (OCDE, Recommandation du Conseil sur l'intelligence artificielle, OECD/LEGAL/0449 *le*, adopté par le Conseil des Ministres de l'OCDE, le 22 mai 2019, disponible à l'adresse : https://legalinstruments.oecd.org/api/print?ids=648\&lang=fr (consultée pour la dernière fois, le 22 janvier 2021) à propos de la sécurité des traitements utilisant l'IA : *'AI systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety risk. To this end, AI actors should ensure traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle, to enable analysis of the AI system's outcomes and responses to inquiry, appropriate to the context and consistent with the state of art.AI actors should, based on their roles, the context, and their ability to act, apply a systematic risk management approach to each phase of the AI system lifecycle on a continuous basis to address risks related to AI systems, including privacy, digital security, safety and bias.'*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

à d'autres manipulations des données ou des algorithmes. ». On ajoute que tant les textes du Parlement européen, du Conseil de l'Europe que de l'OCDE[121] insistent sur la régularité nécessaire des contrôles de sécurité au vu du fonctionnement évolutif des systèmes d'IA et, sur les obligations des fournisseurs de données et des algorithmes de collaborer à la sécurité du système en particulier par une documentation adéquate et l'intervention en cas de dysfonctionnement des applications.

4.3 De quelques questions relatives au consentement

26. Le consentement du patient face à l'IA – La légitimité des traitements dans le secteur de la santé est souvent fondée sur le consentement[122]. Même si une certaine doctrine accorde au consentement une priorité parmi les autres causes de licéité mentionnées à l'article 6 ou 9 dans la mesure où elle exprime le principe même d'autodétermination qui fonde la protection des données, nous estimons que le consentement figure comme une cause de légitimité parmi les autres proposées par les articles 6 et 9 (intérêt public, intérêts vitaux de la personne concernée, obligations en matière de droit du travail…) et ne bénéficie d'aucune priorité par rapport à ces dernières, même si comme nous l'avons dit (supra, n° 17) dans le cas de la relation du médecin à son patient, le droit du patient à participer aux décisions relatives à sa santé implique le recours au consentement. On note également que l'article 9 exclut en matière de données médicales d'invoquer les nécessités des services offerts contractuellement par cette dernière. Ainsi, la maison de repos ne pourra invoquer les services qu'elle offre contractuellement à ses pensionnaires pour justifier le traitement de données médicales. Même en matière de santé, dans le cadre de la « consumérisation » de services de santé *via* le Net (tel le suivi de la santé dans le cadre de l'installation de systèmes « *self quantified* »), le consentement est parfois obtenu dès la visite d'un site Web par l'acceptation de cookies, selon la formule souvent trompeuse à moins qu'elle ne soit ironique, des opérateurs de ces sites : « *Nous sommes soucieux de votre vie privée* ». De telles pratiques sont-elles valables ?

Le RGPD exige que ce consentement soit libre, éclairé et spécifique et non ambigu[123]. Il suppose que la personne dispose d'une réelle liberté de choix : « *The reliance on consent should be confined to cases where the individual subject has a genuine free choice and is subsequently able to withdraw the consent without detriment.* »[124]. En particulier, "*when the participant is not in good health conditions, consent will not be*

[121] OCDE, Recommandation du Conseil sur l'intelligence artificielle, OECD/LEGAL/0449 *le*, adopté par le Conseil des Ministres de l'OCDE, le 22 mai 2019, disponible à l'adresse : https://legalinstruments.oecd.org/api/print?ids=648\&lang=fr (consultée pour la dernière fois, le 22 janvier 2021).

[122] Même si certaine doctrine accorde au consentement une priorité parmi les autres causes de licéité mentionnées à l'article 6 ou 9 dans la mesure où elle exprime le principe même d'autodétermination qui fonde la protection des données », nous estimons que le consentement figure comme une cause de légitimité parmi les autres proposées par les articles 6 et 9 (intérêt public, intérêts vitaux de la personne concernée, obligations en matière de droit du travail, … et ne bénéficie d'aucune priorité par rapport à ces dernières. On note cependant que l'article 9 exclut en matière de données médicales d'invoquer les nécessités des services offerts contractuellement par cette dernière.

[123] Groupe de travail de l'article 29, « *Lignes directrices sur le consentement au sens du règlement 2016/679* », Adoptées le 28 novembre 2017, Version révisée et adoptée le 10 avril 2018. Sur ces conditions, on se référera aux développements de BEAUCHAMP et CHIDRESS (Principles of biomedical ethics, *op. cit.*, p. 140 et s.) Pour ces auteurs, le consentement est l'expression suprême de l'autonomie du sujet.

[124] Groupe de travail de l'article 29 sur le traitement des données relatives à la santé dans les dossiers électroniques de santé, 15 février 2007, WP. 131.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

the appropriate legal basis in most cases »[125]. Le consentement émane de la personne concernée ou de son représentant, notamment si la personne est mineure ou si, par une déficience mentale voire physique notamment due à l'âge, elle ne peut exprimer un consentement éclairé. A cet égard, le fait que le consentement émanera alors de la personne de confiance choisie *in tempore non suspecto* par l'« incapable », n'empêche pas que ce dernier doit être informé et participer tant que faire se peut à la décision de consentir[126]. L'article 9 ajoute qu'en matière de données médicales, génétiques ou biométriques, le consentement doit être « explicite », c'est-à-dire requérir une action positive. Ces exigences nécessitent que l'accord du patient ou de la personne concernée doive figurer de manière distincte du consentement donné de manière générale et ne comporter aucune ambiguïté. Pour prendre un exemple, au cas où votre accord à voir traiter vos données à caractère personnel aux fins d'une recherche médicale ou de votre suivi de santé est demandé par voie électronique, il ne suffira pas de se contenter d'une information qui explique que le fait de remplir un questionnaire suffit pour valider le traitement (consentement non ambigu), il sera requis en outre que le responsable du traitement ajoute un *pop up* sur lequel la personne concernée est invité à indiquer son consentement '*Par ce clic, je marque mon accord au traitement …* »[127].

Par ailleurs, on rappelle que l'article 7 du RGPD s'applique même aux traitements de données médicales. On en rappelle la teneur : « 1. *Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant. 2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante. 3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement. 4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.* ».

27. Le consentement, une réalité ou une illusion ? - La complexité des montages que nécessitent les systèmes supportés par les technologies de l'IA, la diversité des sources utilisées, l'impossibilité de prévoir les corrélations qui seront à la base des décisions du responsable et, dans le contexte de l'accès à des services de conseils 'médicaux'

[125] EDPB, Opinion 3/2019 concerning the questions and answers on the interplay between the Clinical trials Regulation (CTR) and the GDPR, 23th of January 2019, p. 4.

[126] En ce sens, à propos des seuls mineurs certes, la Recommendation n° 15.1 des Nations-Unies sur la protection et l'utilisation des données de santé (4 octobre 2019) » *the child has the right to be informed and consideration must be given in the ability of the child to fully understand consequences of processing, and any applicable laws.* ».

[127] A ce sujet, les lignes directrices du Groupe de travail de l'article 29 sur le consentement sous le Règlement 2016/679 (WP257, adopté le 10avril 2018), p. 18.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

gratuits à portée d'un clic, la difficulté de prendre le recul nécessaire au moment du consentement, tous ces facteurs rendent les conditions mises par le RGPD complétement illusoires. Par ailleurs, les circonstances dans lesquelles le consentement est demandé, notamment dans le cas d'intervention médicale mais également en ce qui concerne l'accès à une maison de repos ou l'offre de soins à domicile, la pression exercée sur les patients est telle que l'on peut difficilement parler de consentement libre. Le pouvoir de discuter des personnes concernées prises individuellement et le déséquilibre informationnel de chacun d'eux pèsent peu face à la puissance informationnelle des responsables de traitement et l'opacité du fonctionnement des systèmes. Que proposer dès lors ? Sans doute, et ces solutions ont notre préférence, faut-il prescrire, là où c'est possible et suivant l'exemple du droit de la consommation et en fonction des traitements en cause, un modèle de consentement collectivement négocié entre, d'une part, à la fois le responsable du traitement, les représentants des associations professionnelles (par exemple, les associations des professionnels de santé – éventuellement en fonction des spécialités en cause –, les associations de maisons de repos, enfin, les opérateurs de services utilisant des dispositifs médicaux, …) et, d'autre part, les représentants des patients ou des personnes concernées (par exemple, l'association des personnes atteints de diabète, les associations des personnes victimes de la maladie d'Alzheimer…) Que cette négociation s'accompagne d'une médiation des autorités de protection des données serait sans doute utile.

Au-delà, ne faut-il pas élargir la négociation collective à d'autres points déjà traités ou résultant des droits subjectifs accordés par le RGPD ? Ainsi, la transparence des traitements risque d'être illusoire, si elle n'est qu'individuelle. Ne faut-il pas lui préférer une transparence collective, par la publicité des algorithmes qui permettent le fonctionnement des systèmes IA de santé au moins ceux publics. La négociation (ou du moins la consultation) ne doit-elle pas également sur les informations à communiquer, leur format, les modalités du droit d'accès ou du droit d'opposition et de dialogue suite à une décision automatisée ? La volonté européenne de prôner une co-régulation encadrée[128], c'est-à-dire ayant fait l'objet d'un minimum de concertation entre tous les porteurs d'intérêts légitimes et conforme avec les législations en vigueur pourrait fonder le principe d'une telle négociation. En outre, dans certains cas, il s'agira légalement d'interdire le consentement, et réclamer que seules les autres causes de validité soient invocables suivant l'article 9 du RGPD.

4.4 Les droits de la personne concernée

28. De la transparence initiale comme condition de l'autonomie du patient – Ceci dit, le respect de l'autonomie suppose que l'on donne toute l'information nécessaire à une prise de décision éclairée[129] et que l'on vérifie que cette information est susceptible d'être comprise par le patient ou la personne concernée ou par la personne qu'elle aura désignée pour la représenter. Le RGPD consacre par de multiples dispositions cette condition même de l'autonomie. Dans le domaine de la santé, l'article L1111-2 du

[128] Nous reviendrons sur ce point lors de l'analyse de la proposition de règlement relatif à l'IA.

[129] « *L'accès aux soins de santé requiert dans plusieurs cas d'avoir au préalable accès à l'information appropriée sur son état de santé et sur les services qui peuvent faire l'objet d'un tel accès.* » (V. GAUTRAIS et C. REGIS, « Cybersanté : les tentatives juridiques pour objectiver un domaine en pleine effervescence », in *Mélanges P. MOLINARI,* Ed. Thémis, 2018, p. 209

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

Code de la Santé publique énonce que « toute personne a le droit d'être informé sur son état » et l'article L111-4 selon lequel « toute personne prend, avec le professionnel de santé et compte tenu des informations et des préconisations qu'il lui fournit, les décisions concernant sa santé ». « *Ainsi, deux conditions sont essentielles, estime DAQUIN, la liberté, « comme indépendance vis-à-vis des influences extérieures »*[130] *et l'action possible « comme capacité à agir intentionnellement »*[131]*, par une prise en compte de son consentement. L'information doit amener une compréhension « substantielle » du patient*[132] *»*. Nous ajoutons, sur base du texte de l'article, de telle sorte que le patient participe réellement à la décision qui sera prise.

L'article 12.1 du RGPD précise que « *Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14*[133] *ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens* ». La mise en place souvent bénéfique d'objets intelligents dans l'environnement du patient, en particulier, dans son suivi post-hospitalisation ou d'implants corporels doit faire l'objet d'une information donnée par le responsable du traitement (l'institution hospitalière agissant par le praticien de l'art de guérir ou son délégué), selon les termes de l'article 12. 1 du Règlement. Ainsi, savoir que le pilulier intelligent enregistre votre consommation de médicaments, l'heure de la prise de ces derniers et les éventuels retards à leur prise ne suffit pas. Il est important d'être informé du fait que ce retard est signalé à telle personne ou à tel serveur accessible à telle catégorie et bien évidement que votre droit d'accès s'opère auprès de tel service mis en place par le responsable.

Cette information porte non seulement sur les caractéristiques du traitement mais, au-delà, dans le cas particulier de l'utilisation d'un système d'IA, selon l'article 12. 3 : *« l'existence d'une prise de décision automatisée, y compris un profilage*[134]*, visée*

[130] Tom Beauchamp et James Childress, *Les principes de l'éthique biomédicale*, Médecine et sciences humaines (Belles Lettres, 2018). p. 92.

[131] *Idem.* p. 92.

[132] *Ibid.* p. 51

[133] L'article 13 prévoit que lorsque la collecte est opérée auprès de la personne concernée, les informations suivantes doivent être délivrées : « *a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ; b) le cas échéant les coordonnées du délégué à la protection des données ; c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ; d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ; e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ; et, en cas de flux transfrontières, … »*

[134] Notre rapport relatif au profilage établi pour le Conseil de l'Europe suggère non seulement que l'existence du profilage fasse l'objet d'un sigle facile à repérer mais que la personne puisse en cliquant sur ce sigle disposer d'autres informations, en particulier une information sur l'impact que pourrait avoir le profilage sur la personne concernée. L'article 4. 1 du projet de Recommandation reprend ces informations additionnelles : « *toute information nécessaire à la garantie du caractère loyal du recours au profilage, telle que : – la possibilité, le cas échéant, pour les personnes concernées, de refuser le consentement ou de le retirer, et les conséquences d'un retrait ;*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente_, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée_.

Sans doute, regrettera-t-on que la disposition citée ne prévoit d'obligation relative à la logique sous-jacente que dans le cas de prise de décision entièrement automatisée, lorsqu'on sait que la frontière entre décision totalement automatisée et décision partiellement automatisée est difficile et que le regard confié au praticien de l'art de guérir sur les résultats de l'algorithme leur confère rarement une réelle autonomie de choix, ne serait-ce que par crainte de la responsabilité que ce dernier risque d'encourir s'il remet en cause la 'vérité' sortie de l'ordinateur. Sans doute, l'utilisation du concept de « logique sous-jacente » pose difficulté là où les systèmes de « *machine learning* » travaillent de manière agrégationnelle et opaque ? Faut-il dès lors ne pas appliquer la disposition ? Il nous paraît que cette disposition doit s'appliquer même si la notion d'« *information utile* » reste floue et que le caractère de « *deep learning* » de systèmes d'IA rend l'obligation du responsable difficile à appliquer d'autant plus que le fonctionnement des logiciels d'IA sont, vu leur caractère évolutif, peu transparents, y compris pour les responsables de traitement[135]. On note qu'il s'agit d'une information sur le système et non sur les résultats de l'application à la personne concernée. Pour le reste, il importera que le secteur médical précise sous le contrôle des autorités de protection des données la compréhension de la disposition et définisse des '*best practices'* en la matière. En matière d'IA de type agrégationnel, la recommandation du Conseil de l'Europe en matière de profilage parle d'obligation d'information non pas sur la logique mais sur le 'modèle » suivi par le traitement utilisant l'IA. La notion y est définie comme « *une abstraction mathématique utilisée dans les méthodes d'apprentissage automatique qui fournit une description simplifiée des données pour résoudre la tâche à effectuer* ». Ainsi, même si la description du modèle (cela peut être un arbre de décision, une liste des paramètres auxquels un poids relatif a été accordé suite aux tests sous réserve de l'évolution possible, …) ne suit pas un parcours au sens strict logique, la personne a, néanmoins, droit à obtenir une explication intelligible et donc causale de ce qui permettra à la machine d'établir des résultats et ce, de manière sans doute non aussi précise qu'en cas d'IA symbolique.

Autres difficultés d'application du prescrit du RGPD en matière d'obligation d'information : donner la liste des données ou des catégories de données collectées n'est pas simple lorsque les *big data* utilisées s'enrichissent chaque jour de nouvelles sources et de nouvelles données et il sera utile dès lors de prévoir une mise à jour régulière de

– les personnes ou les organismes auprès desquels d'autres données à caractère personnel sont ou seront collectées ;
– le caractère obligatoire ou facultatif de la réponse aux questions utilisées pour collecter les données personnelles, et les conséquences pour les personnes concernées d'un défaut de réponse ;
– la durée de conservation des données personnelles ;
– le cas échéant, l'impact potentiel du profilage sur la personne concernée ;
– des informations utiles sur le raisonnement qui sous-tend le profilage ou le modèle utilisé par le responsable du traitement des données ».

[135] Ce caractère non transparent des algorithmes d'IA est au cœur des difficultés dénoncées par la CNIL, dans son étude de décembre 2017 disponible sur le site de la CNIL : « *Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle* », qui met en exergue la difficulté dès lors y compris pour le responsable et a fortiori pour la personne concernée de conserver une quelconque maîtrise des traitements qui les utilisent.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

l'information donnée sur le site de référence de description du traitement de profilage. La même remarque vaut pour les 'destinataires' tantôt des données collectées, tantôt des résultats du traitement d'IA et ce, au vu de la complexité des réseaux dans lesquels circule ou circulera l'information. Les recommandations sur l'éthique de l'IA de l'OCDE[136] proposent une approche plus fonctionnelle (mais également plus sujette à interprétations) de l'étendue de l'obligation d'information, lorsqu'elles concernent un système de profilage utilisant l'IA (Recommandation 1.3 : 'transparence et explicabilité') : « *Les acteurs de l'IA devraient s'engager à assurer la transparence et une divulgation responsable des informations liées aux systèmes d'IA. À cet effet, ils devraient fournir des informations pertinentes, adaptées au contexte et à l'état de l'art, afin :*

- de favoriser une compréhension générale des systèmes d'IA,
- d'informer les parties prenantes de leurs interactions avec les systèmes d'IA, y compris dans la sphère professionnelle,
- de permettre aux personnes concernées par un système d'IA d'en appréhender le résultat, et,
- de permettre aux personnes subissant les effets néfastes d'un système d'IA de contester les résultats sur la base d'informations claires et facilement compréhensibles sur les facteurs, et sur la logique ayant servi à la formulation de prévisions, recommandations ou décisions. ».

29. De la transparence au moment de la décision – A cette information lors de la collecte des données tant auprès du patient que d'un tiers, s'ajoute la nécessité d'une information au moment où le responsable de traitement communique la décision tirée de l'application du système IA L'article 22 du RGPD qui consacre le droit de la personne concernée « *de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* », appelle les remarques suivantes. L'analyse de cette disposition laisse apparaître nombre de lacunes ou, en tout cas, d'ambiguïtés. *Que veulent dire les expressions : 'décision fondée exclusivement' ; « affecter de manière significative » et le terme « uniquement » ?* Selon certains auteurs, au vu de la difficulté pour le praticien de s'écarter de la recommandation de la machine, le patient devrait être informé qu'une décision s'appuie sur une recommandation algorithmique, quand bien même cette dernière n'apporterait qu'une aide à la décision du diagnosticien[137]. Au regard de l'article 11 du projet de loi bioéthique, le législateur partage cette position[138]. *Enfin, la décision dont parle l'article 22 doit viser une « personne concernée ». C'est la conséquence certes d'une*

[136] OCDE, *Recommendation on Artificial Intelligence (AI) – the first intergovernmental standard on AI* –, adopté par le Conseil des Ministres de l'OCDE, le 22 mai 2019.

[137] E. NERI *et al.*, « Artificial Intelligence : Who Is Responsible for the Diagnosis ? », *La Radiologia Medica*, 125, n° 6 (juin 2020) : 517-21, https://doi.org/10.1007/s11547-020-01135-9. p. 520 ; T. JACQUES, L. FOURNIER et alii, « Proposals for the Use of Artificial Intelligence in Emergency Radiology ». *Diagnostic and Interventional Imaging*, 2 décembre 2020, p. 4.

[138] « *L. 4001-3. – I. – Lorsque, pour des actes à visée préventive, diagnostique ou thérapeutique, est utilisé un traitement algorithmique dont l'apprentissage est réalisé à partir de données massives, le professionnel de santé qui décide de cette utilisation s'assure que la personne concernée en a été informée au préalable et qu'elle est, le cas échéant, avertie de l'interprétation qui en résulte.* ». Sénat, « Projet de loi relatif à la bioéthique », Pub. L. No. 53 (2021). art.11.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

législation centrée sur la protection de personnes individuelles mais ne faudrait-il pas également prendre en compte le fait que des systèmes en particulier prédictifs visent des catégories de personnes : ainsi les personnes habitant tel quartier, ayant tel type de comportement sur le net, telle mobilité… ? Le risque est ici collectif et, de ce fait, mériterait a fortiori d'être pris en compte. Nous ne pourrons dans le cadre de cette contribution analyser tous ces ambigüités[139]*. Par ailleurs, l'article 22.2 prévoit des exceptions qui s'appliqueront à la plupart des systèmes d'IA : besoins contractuels ou précontractuels, consentement de la personne concernée ou exécution d'une mission d'intérêt public autorisée par l'Etat. Manque l'hypothèse d'un système d'IA dont la licéité reposerait sur un intérêt légitime prépondérant du responsable du traitement.*

30. Du droit à l'explication en cas de décision médicale automatisée – L'article 22.3 réclame au cas où les exceptions à l'interdiction de prise de décision sur base exclusive d'un traitement automatisé[140] *s'appliqueraient, que le responsable mette « en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement d'exprimer son point de vue et de contester la décision* ». Au-delà, la personne concernée peut-elle avoir accès à une explication par écrit ou, à défaut, orale des critères utilisés pour justifier la décision et de leur application à son cas concret ? L'article 22[141] ne le réclame pas. La disposition évoque simplement le droit à des 'mesures appropriées' et à l'obtention d'une intervention humaine. *Certes, l'intervention humaine ne peut se limiter à une simple réaffirmation par oral de la 'vérité sortie de l'ordinateur' mais à partir de quand pourra-t-on considérer que l'humain a une réelle capacité de remise en cause de la présomption de vérité sortie des ordinateurs*[142] *? Que recouvrent les termes 'garanties appropriées' : le droit à une audience en face à face ? Un droit de contestation de la décision après explication ? Les 'garanties appropriées' exigent-t-elles, par exemple, que le praticien de l'art de guérir, sans doute une fois l'anamnèse bouclée sur base des déductions de l'IA, explique le raisonnement suivi qui a amené à l'intervention chirurgicale. N'est-il pas trop tard ? Nonobstant le flou de l'article 22 et la difficulté due à l'opacité des systèmes complexes d'IA,* le considérant n° 71 qui lui est lié exige que le bénéfice de ces exceptions de l'article 22.2 soit assorti par ceux qui s'en prévalent « *de garanties appropriées, qui devraient comprendre une information spécifique de la*

[139] Sur cette analyse, nous renvoyons à notre ouvrage : *Le RGPD face aux défis de l'intelligence artificielle,* Cahier du CRIDS, n° 48, Larcier, Bruxelles, 2020, p. 109 et s., n° 35 et s. et les différentes références y reprises.

[140] RGPD, Article 22.2 : « *2. Le paragraphe 1 ne s'applique pas lorsque la décision :*
a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;
b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou
c) est fondée sur le consentement explicite de la personne concernée. » (nous soulignons).

[141] Le considérant n° 71 semble par contre le réclamer comme nous le dirons dans l'alinéa qui suit.

[142] Sur cette'incontestabilité' de la décision produite par la machine, lire entre autres, M. KAMINSKY : "*And where human decision-making can often be contested, algorithmic decision-making […] is often taken at face value, and left unchallenged and unchallengeable.* ». ("Binary governance : lessons from the GDPR's approach to algorithmic accountability", *Southern California Law Review*, 2019, 76, p. 15. Il semble que les autorités singapouriennes exigent que les personnes charges de répondre aux demandes d'explication ou de contestation des décisions d'applications de '*machine learning'* disposent d'une réelle compétence en matière *de machine learning* et connaissent l'application

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable,* Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision » . *Ainsi,* le responsable se devra, suite à une décision prise, d'offrir, non seulement, une interface humaine capable de recevoir la personne concernée et de répondre à ses questions mais également de donner toutes les informations qu'il détient dans le cadre des exigences d"explicabilité' de la décision prise[143], c'est-à-dire au minimum les bases suffisantes pour permettre la compréhension du processus, qui a mené à la décision prise, et la possibilité, dès lors, pour la personne concernée, de la contester en connaissance de cause. Cette possibilité de contester doit s'entendre de la possibilité d'un recours à l'autorité certes, mais surtout d'un recours interne par une personne ayant compétence de revoir les décisions prises par ou à la suite de l'utilisation du système de *machine learning.* L'ensemble de ces obligations est repris aux points 5.6 et s. de la recommandation du Conseil de l'Europe sur le profilage déjà citée : *« … Lorsque le système de traitement de profilage émet une décision ou un projet de décision, il est fortement recommandé que :*

les responsables du traitement tiennent compte de toutes les particularités des données et ne se fondent pas simplement sur des informations ou des résultats du traitement pris hors de son contexte ;

en cas de traitement de profilage à risque élevé, le responsable du traitement informera la personne concernée des opérations algorithmiques qui sous-tendent le traitement de données, y compris les conséquences pour elle de ces opérations. Dans ce cas, l'information doit être telle qu'elle permette à la personne concernée de comprendre la justification des décisions ou propositions de décision prises à son encontre. Cette exigence dépend fortement des conséquences que peut avoir l'impact du résultat obtenu pour la personne concernée, conformément au principe d'explicabilité ;

dans ce cas, la personne nommée par le responsable du traitement doit pouvoir, sur la base d'arguments raisonnables, décider de ne pas se baser sur les résultats des recommandations découlant de l'utilisation du traitement de profilage ;

en présence d'indications permettant de penser qu'il y a eu discrimination directe ou indirecte fondée sur le fonctionnement du traitement de profilage, les responsables du traitement et les sous-traitants apportent la preuve de l'absence de discrimination..

Les personnes affectées par une décision fondée sur un traitement de profilage devraient avoir le droit de recevoir toute explication utile sur cette décision, ou la proposition de décision, afin d'en comprendre la justification. La propriété intellectuelle ou l'existence de secrets commerciaux ne peuvent être contestées que lorsque les informations à fournir affecteraient gravement ces droits. L'invocation de ces droits et intérêts par le responsable du traitement ne peut conduire à priver la personne concernée ou le groupe concerné de la capacité de comprendre les décisions ou les projets de décision

[143] Comme l'affirme le Groupe de l'article 29 dans ses Lignes directrices reprises et confirmées par l'European Data Protection Board (Groupe de l'article 29, *Lignes directrice relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, WP251 rev.01, adoptées le 3 octobre 2017 et révisées le 6 février 2018, p. 18), « *compte tenu du principe fondamental de transparence qui sous-tend le RGPD, les responsables du traitement doivent veiller à expliquer clairement et simplement aux personnes concernées la manière dont fonctionne le profilage ou le processus décisionnel automatisé* », ce qui ne signifie pas « *une explication complexe des algorithmes utilisés* »

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

adoptés. Nonobstant le recours devant l'autorité de contrôle ou le recours juridique, les personnes concernées devraient avoir le droit de contester le profilage devant une personne désignée par le responsable du traitement, ayant accès à toutes les informations sur le profilage et son fonctionnement et compétente pour modifier ou supprimer la décision ou le projet de décision. ».

31. L'obligation de 'Privacy Impact Assessment' et l'IA – La notion de traitement « à risques élevés » – En cas de traitements dits à haut risque, l'article 35 du RGPD impose des obligations particulières d'évaluation. Dans la mesure où nombre de systèmes d'IA traitant des données à caractère personnel constituent des traitements à haut risque, le régime particulier prévu par le RGPD et l'analyse des critères possibles de présence de ces 'hauts risques' doivent être abordés.

Commençons par l'article 35.1 du RGPD qui sert de point de départ à la réflexion de nombre de documents réclamant l'évaluation des systèmes d'IA. Il énonce : "*Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* »[144] La notion de 'risque élevé 'est donc au centre de la décision européenne de réglementer plus sévèrement certains traitements en imposant à leurs responsables cette obligation particulière d'évaluation des risques. Il ne s'agit pas ici de nous livrer à une analyse exhaustive des deux articles du RGPD qui introduisent le PIA dans l'arsenal des dispositions de protection des données, le Groupe de l'article 29 a proposé cette analyse systématique des dispositions[145], mais de relever les points essentiels à notre propos. L'analyse d'impact est imposée (article 35.1.) lorsque le traitement présente un « *risque élevé* », « *en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement* ». La priorité accordée au critère « du recours aux nouvelles technologies »[146] mérite d'être soulignée. Elle indique clairement que les auteurs du RGPD était d'emblée conscients de la nécessité d'une évaluation des applications générées par les technologies alors émergentes, telles l'IA comme la reconnaissance faciale et largement utilisées en matière de profilage. L'article 35.3 décrit un certain nombre de traitements pour lesquels l'analyse est requise[147] et, au-delà, délègue, aux autorités nationales de protection[148] sous le contrôle et la coordination du CEPD, le soin de

[144] L'article 27.1. de la directive européenne dite 'Police' reprend le même libellé

[145] G.29, *Lignes directrices du 4 octobre 2017 concernant l'analyse d'impact relative à la protection des données et la manière de déterminer si le traitement « est susceptible de 'engendrer un risque élevé » aux fins du Règlement 2016/679,* WP. 248, Rev. 01 confirmées par le CEPD, successeur du Groupe de l'article 29. Le lecteur se référera également utilement aux commentaires du RGPD, ainsi, celui publié par T. DOUVILLE, *Droit des données à caractère personnel,* Gualino, Lextenso, 2021, p. 227 et s.

[146] Souligné par le considérant n° 91. Voir aussi les lignes directrices du G.29 (p. 12) qui précise que dans ce cas le risque est accru du fait que ces nouvelles technologies de collecte (Internet des objets) et d'utilisation des données peuvent avoir des conséquences personnelles ou sociales inconnues

[147] Ainsi, pour les traitements ayant pour finalité l'évaluation ou la surveillance systématique de la personnalité ou pour objet des données sensibles collectées à grande échelle de données sensibles et donc de données médicales, génétiques ou biométriques

[148] Ainsi, la CNIL a ajouté *nombre de traitements recourant à des données de santé(traitements par les établissements de santé ou médico sociaux pour la prise en charge des personnes, traitements portant sur les données génétiques de personnes vulnérables, traitements permettant la constitution d'un entrepôt*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

fixer et publier une liste positive et négative des traitements soumis ou non à l'obligation[149]. On ajoute que les listes retenues par le RGPD et par les autorités de contrôle ne sont pas exhaustives ; Comme le note le G. 29[150], « *d'autres opérations pouvant bien évidemment présenter un risque aussi élevé* ».

Il s'agit, dans le cadre du RGPD, de « risques pour les droits et libertés des personnes concernées », en d'autres termes, ceux que le RGPD entend protéger suivant l'article 1.2. Pour DOUVILLE, mais son interprétation large est contestable, l'expression pourrait recouvrir, « *au-delà du droit au respect de la vie privée et à la protection des données à caractère personnel, la liberté de circulation, l'égalité et l'absence de discrimination, le droit à la santé, la liberté d'entreprendre ou le droit au respect des biens* »[151]. On retrouve, à l'appui de cette interprétation large, la volonté de la Commission LIBE du Parlement d'apporter, lors de la discussion relative à l'adoption du RGPD, un amendement incluant spécifiquement les risques de discrimination dans le champ des risques créés par les traitements. BIRNNS[152] note que cet amendement a été rejeté par la suite mais ajoute que le considérant 75 mentionne toujours ce risque. Bref, il est difficile de déterminer à l'heure actuelle si, dans le cadre de l'article 35 du RGPD, les questions d'égalité et de discrimination doivent être prises en considération lors de l'évaluation de la potentialité du risque lié au traitement de données. Ce point est important dans la mesure où d'autres risques que les seuls risques subis individuellement d'atteinte à nos libertés sont en jeu dans le développement des applications d'intelligence artificielle, en particulier en matière de santé. Cette réflexion sur le besoin d'élargir le champ de la réglementation à la prise en compte des risques de non-respect de la dignité à reconnaître à chaque être humain, de discrimination et, plus largement, d'atteinte à la justice sociale (voir supra, n° 16 et 17) voire des risques sociétaux, conduit à nous interroger sur les deux autres textes européens. Enfin, on

---

de données ou d'un registre, traitement de données biométriques pour la reconnaissance de personnes incluant des personnes vulnérables, traitements permettant la constitution d'un entrepôt de données ou d'un registre, traitement de données biométriques pour la reconnaissance de personnes incluant des personnes vulnérables). Dans le domaine du médico-social, sont également concernés les traitements ayant pour finalité l'accompagnement social ou médico-social des personnes et les traitements ayant pour finalité la gestion de l'alerte et le signalement dans le domaine social et sanitaire. »(CNIL, délibération du n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise)

[149]Ainsi, la CNIL a établi deux listes (CNIL, délibération n° 2018-326 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données prévues par le RGPD. (Sur ces deux listes, lire le commentaire d'A. DEBET et N. METALLINOS in *Comm. Comm electr.* Janvier 2019). Ces lignes directrices ont fait l'objet, le 25 septembre 2018, de l'avis 9/2018 du CEPD.

[150]G.29, Lignes directrices déjà citées, p. 10. Le G. 29 énumère pas moins de 9 critères qui devraient être pris en compte dans cette évaluation du risque et considère que la présence de deux de ces critères doit aboutir à la conclusion de la présence d'un risque élevé. Sur ce point, les commentaires de N. METALLINOS, « Consécration du rôle central des études d'impact sur la vie privée », *Comm.com électr.*, 2017, comm. 57 et Y. POULLET, "The data protection impact assessment or rather the Privacy Impact Assessment, a revolution with a future in the age of artificial intelligence ?" in "Un droit de l'intelligence artificielle : entre règles sectorielles et régime général. Perspectives comparées", sous la direction de C. CASTETS et J. EYNARD, Ottawa- Toulouse, à paraître.

[151]T. DOUVILLE, *op. cit.*, n° 479, p. 228. On note que le Groupe dit de l'article 29, dans ses lignes directrices relatives au DPIA du 4 avril 2017 déjà citées, se réfère également, mais de manière incidente, aux risques de discrimination : « *As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.*"

[152]R. BIRNNS, "Data Protection impact assessment : a meta regulatory approach », *Int. data &Privacy Law„* 2017, vol. 7, p. 28.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

note que les premières versions du RGPD requerraient l'avis des personnes concernées lors de l'évaluation. L'article 35. 6 n'envisage désormais cet avis que « *le cas échéant* » et « *sans préjudice de la protection des intérêts généraux ou commerciaux ou publics ou de la sécurité des opérations de traitement* »[153].

5 Le règlement de 2017 sur les dispositifs médicaux

32. La notion de dispositif médical applicable aux systèmes d'intelligence artificielle ? – L'intervention de l'Internet des objets, d'implants corporels, l'utilisation de systèmes 3D, la présence multipliée de robots pose la question de la qualification de tous ces outils qui, tantôt servent à nourrir les systèmes d'intelligence artificielle, tantôt fonctionnent grâce à cette dernière ; ils soulèvent la question délicate de leur qualification aux yeux de la réglementation. S'agit-il dans tous ces cas de dispositifs médicaux ? La réponse à la question est loin d'être sans conséquence. Les dispositifs médicaux dans lesquels s'intègrent les systèmes d'intelligence artificielle sont en effet réglementés par un règlement de l'Union européenne du 5 avril 2017[154]. L'article 2 1) définit comme suit le *« dispositif médical », tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales précises suivantes : diagnostic, prévention, contrôle, pronostic, traitement ou atténuation d'une maladie, diagnostic, contrôle, traitement, atténuation d'une blessure ou d'un handicap ou compensation de ceux-ci, investigation, remplacement ou modification d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique, communication d'informations au moyen d'un examen in vitro d'échantillons provenant du corps humain, y compris les dons d'organes, de sang et de tissus, et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. » Cette définition large couvre également les dispositifs réalisés sur mesure. On note que les outils logiciels y compris d'intelligence artificielle agissant à distance et destinés au fonctionnement d'un dispositif médical sont réputés*

[153] A noter de manière plus explicite, le texte déjà cité de la Recommandation du Conseil de l'Europe en matière de profilage (point 7.9) : « *Aux fins d'une évaluation continue des risques tant individuels que collectifs et, en tout cas lorsqu'il s'agit de traitements de profilage à risque élevé, les responsables du traitement et, le cas échéant, les sous-traitants devraient documenter l'entraînement du modèle et effectuer des évaluations d'impact régulières en traitant des risques spécifiques du profilage fondé sur des systèmes d'IA. Pour atteindre cet objectif, ils devraient s'entourer d'une équipe d'évaluation multidisciplinaire et consulter les représentants des intérêts concernés par le profilage, y compris les personnes faisant l'objet d'un profilage. Ce processus d'évaluation devrait être mené par des personnes dotées des qualifications professionnelles et des connaissances adéquates pour apprécier les différents impacts, y compris dans leurs dimensions juridique, sociale, éthique et technique.* »

[154] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE. Dans son Livre Blanc de 2015 : « De la e-santé à la santé connectée »44, le Conseil national de l'ordre des médecins prône de même à propos des objets connectés et implants corporels, une régulation par des déclarations de conformité aux standards européens, standards qui tiendraient compte de la nécessité d'information des patients et des exigences en matière de sécurité tant du matériel, des logiciels, de la communication et au-delà de la protection des données

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

« dispositif actif » soumis au règlement[155]*, de même que les implants corporels*[156]*. La Cour de Justice de l'Union européenne*[157] *n'a pas hésité à considérer qu'un logiciel relève du champ d'application de la directive et donc aujourd'hui du Règlement s'il est utilisé dans un contexte médical et que sa destination, définie par le fabricant, est spécifiquement médicale. La Cour*[158] *a même précisé à propos de logiciel d'aide à la prescription qu'« un logiciel dont l'une des fonctionnalités permet l'exploitation de données propre à un patient aux fins notamment de détecter des contre-indications, les interactions médicamenteuses et les posologies excessives, constitue, pour ce qui est de cette fonctionnalité, un dispositif médical, et ce même si un tel logiciel n'agit pas directement dans ou sur le corps humain. ».*

33. Le Règlement 2017/745 sur les dispositifs médicaux – un premier pas vers l'*Ethical design* – Le Règlement déjà cité remplace des directives déjà anciennes de 1993[159]. Sans pouvoir, dans le cadre de cet article, détailler les prescrits de ce Règlement fleuve, relevons (article 5) qu'« *un dispositif ne peut être mis sur le marché ou mis en service que s'il est conforme au présent règlement au moment où il est dûment fourni et dès lors qu'il est correctement installé, entretenu et utilisé conformément à sa destination.* ». L'annexe 1 du Règlement précise : *« Les dispositifs atteignent les performances prévues par leur fabricant et sont conçus et fabriqués de telle manière que, dans des conditions normales d'utilisation, ils soient adaptés à leur destination. Ils sont sûrs et efficaces et ne compromettent pas l'état clinique ou la sécurité des patients ni la sécurité ou la santé des utilisateurs ou, le cas échéant, d'autres personnes, étant entendu que les risques éventuels liés à leur utilisation constituent des risques acceptables au regard des bénéfices pour le patient et compatibles avec un niveau élevé de protection de la santé et de la sécurité, compte tenu de l'état de l'art généralement admis ».* Cette obligation implique que les logiciels d'intelligence artificielle contenus dans les dispositifs médicaux et, de manière plus large, l'ensemble des éléments qui en permettent le fonctionnement, fassent l'objet d'essais et contrôles[160] qui permettent

[155] Art. 2. 4) : « *« dispositif actif », tout dispositif dont le fonctionnement dépend d'une source d'énergie autre que celle générée par le corps humain à cette fin ou par la pesanteur et agissant par modification de la densité de cette énergie ou par conversion de celle-ci…. Les logiciels sont aussi réputés être des dispositifs actifs* »

[156] Art. 2.5) : *« « dispositif implantable », tout dispositif, y compris ceux qui sont absorbés en partie ou en totalité, destiné :*
- à être introduit intégralement dans le corps humain, ou
- à remplacer une surface épithéliale ou la surface de l'œil,
par une intervention clinique et à demeurer en place après l'intervention.

[157] CJUE, 22 novembre 2012, aff. C-219/11, Brain Produucts GmBH c. Biosemi et alii, considérants 16 et 17.

[158] CJUE 7 décembre 2017, aff. C.329/16, SNITEM et Philips France c. Premier Ministre, Considérant 21.

[159] Le Règlement JOUE, L.117/165, 5 mai 2017) remplace les deux directives 90/385 et 93/43 relatives au même objet. On note qu'il s'agit d'un Règlement et non plus d'une Directive, qu'il contient 178 pages contre environ une soixantaine pour les Directives citées ; qu'il est composé de 10 chapitres et de 17 annexes.

[160] « *Les investigations cliniques sont conçues, autorisées, conduites, documentées et notifiées conformément aux dispositions du présent article et des articles 63 à 80, des actes adoptés en vertu de l'article 81, et de l'annexe XV lorsqu'elles sont effectuées, dans le cadre de l'évaluation clinique en vue de l'évaluation de la conformité, aux fins de l'un des objectifs suivants : » a) établir et vérifier que, dans des conditions normales d'utilisation, un dispositif est conçu, fabriqué et conditionné de manière à convenir à l'une ou plusieurs des fins énumérées à l'article 2, point 1), et qu'il atteint les performances prévues, telles qu'elles sont spécifiées par son fabricant ; b) établir et vérifier les bénéfices cliniques d'un dispositif, tels qu'ils sont spécifiés par son fabricant ; c) établir et vérifier la sécurité clinique du dispositif et détecter les éventuels effets secondaires indésirables dans des conditions normales d'utilisation du dispositif et évaluer si ceux-ci constituent un risque acceptable au regard des bénéfices attendus du dispositif concerné. ». On notera le rapprochement entre cette exigence d'évaluation interne des dispositifs médicaux et celle exigée en matière de systèmes d'intelligence artificielle (voir infra, n° 31).*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

de vérifier que, selon l'article 61, il est conforme aux exigences des prescrits européens, en particulier en matière de qualité, de protection de la santé, de sécurité et de non-dommage aux personnes. Ces procédures d'évaluation seront plus ou moins strictes, internes au fabricant ou confiées à un organisme notifié[161], suivant la classe (quatre classes) dont relève le dispositif en question et ce « *en fonction d'une part de la destination des dispositifs et des risques qui leur sont inhérents* » (article 51). L'article 51 du Règlement sur les dispositifs médicaux dont la portée large a été soulignée (*supra, n° 32)* répartit les objets visés en classe I, classe IIa, classe IIb et classe III en fonction de la destination des dispositifs et des risques qui leur sont inhérents[162]. La classification est effectuée conformément à l'annexe VIII. Ainsi, parmi de nombreuses autres catégories, cette annexe énonce que « *Tous les dispositifs actifs destinés à commander, à contrôler ou à agir directement sur les performances des dispositifs implantables actifs relèvent de la classe III* » (art. 6.1. Règle 9) et, plus loin, que « *les logiciels destinés à fournir des informations utilisées pour prendre des décisions à des fins thérapeutiques ou diagnostiques relèvent de la classe IIa, sauf si ces décisions ont une incidence susceptible de causer :*

- la mort ou une détérioration irréversible de l'état de santé d'une personne, auxquels cas ils relèvent de la classe III, ou
- une grave détérioration de l'état de santé d'une personne ou une intervention chirurgicale, auxquels cas ils relèvent de la classe IIb.

Les logiciels destinés à contrôler des processus physiologiques relèvent de la classe IIa, sauf s'ils sont destinés à contrôler des paramètres physiologiques vitaux, lorsque des variations de certains de ces paramètres peuvent présenter un danger immédiat pour la vie du patient, auxquels cas ils relèvent de la classe IIb. Tous les autres logiciels relèvent de la classe I » (article 6.2. Règle 10). Cette approche fondée sur la finalité des dispositifs et les risques associés (*Risk-based approach*) permet de définir des types et degrés de contrôle variable suivant le niveau de risque. A noter que le règlement précise (article 62) à propos de ce devoir d'expérimentation : *« Les investigations cliniques sont conçues et conduites de manière à garantir la protection des droits, de la sécurité, de la dignité et du bien-être des personnes y participant, à faire prévaloir ces considérations sur toute autre et à garantir la validité scientifique, la fiabilité et la*

[161] Voir l'article 35. 1. sur le principe de l'existence de ces organismes notifiés « *Tout État membre qui entend désigner un organisme d'évaluation de la conformité en tant qu'organisme notifié, ou a désigné un organisme notifié, pour mener des activités d'évaluation de la conformité en application du présent règlement nomme une autorité (ci-après dénommée « autorité responsable des organismes notifiés »), qui peut être composée d'entités constituantes distinctes en vertu de la législation nationale et est chargée de la mise en place et du suivi des procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et du contrôle des organismes notifiés, ainsi que de leurs sous-traitants et filiales. ».* Le statut, les exigences, les responsabilités et les interventions de ces organismes notifiés sont longuement décrits dans le Règlement.

[162] A cet égard, voir les excellents tableaux repris dans l'étude COCIR ("AI in EU medical device legislation", Sept 2020, p. 29) : "*The vast majority of medical device software is class IIa or higher under the EU MDR or class B or higher under the EU IVDR, requiring an ex ante and ex post conformity assessment by a notified body. Figure 9 Classification Rule 11 1 is based on the IMDRF SaMD risk framework. This risk framework considers the significance of the information (x-axis) and the criticality of the disease or condition (y-axis) to assess the risk of software.*"

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

robustesse des données cliniques qu'elles génèrent ». Par ailleurs, seul le consentement éclairé[163] autorise la participation d'un patient ou d'une personne à l'expérimentation.

En ce qui concerne le contrôle, le Règlement impose un contrôle interne similaire à celui prévu par le RGPD. L'article 15 énonce : « *les fabricants disposent au sein de leur organisation d'au moins une personne chargée de veiller au respect de la réglementation possédant l'expertise requise dans le domaine.* ». Il ajoute à ce premier instrument de contrôle, celui externe par ce qu'il qualifie d'« organisme notifié », soit une organisation désignée par un Etat membre de l'Union européenne pour réaliser l'évaluation d'un produit au regard des exigences européennes et, en cas d'évaluation positive, sa mise sur le marché. A cet égard, on sera attentif à la qualité des données qui auront servi de test ou par la suite enrichiront la connaissance de l'algorithme. Le dispositif, une fois conforme, recevra un IUD (système d'Identification Unique de tous les Dispositifs). Associée au système UDI, une base de données EUDAMED reprend et rend accessibles toutes les informations concernant les dispositifs médicaux, rec ues des fabricants et des organismes notifiés, en ce compris les expérimentations cliniques. Ainsi, la déclaration de conformité[164] (qui se traduit par un marquage CE {conformité européenne}) implique l'enregistrement du dispositif et l'attribution d'un numéro d'identification. L'article 18[165] prescrit les informations que le fabricant doit fournir de manière compréhensible (article 32) à propos du dispositif qu'il met sur le marché. Enfin, le Règlement, dans le cadre de la coopération entre les Etats membres, met en place un groupe de coordination en matière de dispositifs médicaux (GCDM) afin de permettre une meilleure régulation du secteur au niveau européen. Parmi les nombreuses compétences de ce Groupe, on note, l'assistance des Etats membres et de la Commission à la réglementation, l'audit des organismes notifiés, l'élaboration d'orientations pour une application efficace et harmonisée du Règlement. Cet organe est également un relais de communication entre les organismes notifiés et

[163] L'article 1, 55 du Règlement définit comme suit le consentement éclairé : « *consentement éclairé », l'expression, par un participant, de son plein gré et en toute liberté, de sa volonté de participer à une investigation clinique particulière, après avoir pris connaissance de tous les éléments de l'investigation clinique qui lui permettent de prendre sa décision ou, dans le cas des mineurs et des personnes incapables, une autorisation ou un accord de leur représentant légal de les faire participer à l'investigation clinique. ». Comparer avec la définition donnée à la notion par le Règlement de protection des données.3 L'article 63 ajoute : « Le consentement éclairé est écrit, daté et signé par la personne qui effectue l'entretien visé au paragraphe 2, point c), et par le participant ou, si ce dernier n'est pas en mesure de donner son consentement éclairé, par son représentant légal après avoir été dûment informé conformément au paragraphe 2. Si le participant n'est pas en mesure d'écrire, son consentement peut être donné et documenté par d'autres moyens appropriés en présence d'au moins un témoin impartial. Dans ce cas, le témoin signe et date le document relatif au consentement éclairé. «*

[164] « *La déclaration de conformité UE atteste que les exigences du présent règlement ont été respectées pour ce qui est du dispositif concerné. Le fabricant tient à jour la déclaration de conformité UE. La déclaration de conformité UE contient, au minimum, les informations qui figurent à l'annexe IV et est traduite dans une ou des langues officielles de l'Union … » (Article 19 du Règlement)*

[165] « *Le fabricant d'un dispositif implantable joint au dispositif les éléments suivants : a) les informations permettant l'identification du dispositif, dont le nom, le numéro de série, le numéro de lot, l'IUD, le modèle du dispositif, ainsi que le nom, l'adresse et le site Internet du fabricant ; les mises en garde, précautions ou mesures à prendre par le patient ou par un professionnel de la santé à l'égard des interférences réciproques avec des sources ou conditions d'environnement extérieures ou des examens médicaux raisonnablement prévisibles ; c) toute information sur la durée de vie prévue du dispositif et le suivi éventuellement nécessaire ; d) toute autre information destinée à garantir l'utilisation sûre du dispositif par le patient, notamment les informations figurant à l'annexe I, section 23.4, point u). Les informations visées au premier alinéa sont fournies, aux fins de les mettre à la disposition du patient auquel on a implanté le dispositif, par tout moyen permettant un accès rapide à ces informations et elles sont rédigées dans la ou les langues définies par l'État membre concerné. Les informations sont écrites de manière à être aisément comprises par un profane et sont mises à jour »*

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

la Commission dans la mesure où le GCDM sera au centre d'un processus de *reporting* applicable aux dispositifs de classe III.

Le chapitre VI : « Evaluation clinique et investigations cliniques » décrit les processus à mettre en place en particulier pour les dispositifs de classe II et III. On note que selon une étude comparative Etats-Unis et Europe de janvier 2021, portant sur près de 462 dispositifs médicaux basés sur l'apprentissage automatique, sur l'ensemble des 240 algorithmes d'IA en santé répertoriés dans l'Union européenne, 35 % de ces dispositifs médicaux sont de classe I (risques faibles), 40 % de classe IIa (risques potentiels modérés/mesurés), 12 % de classe IIb (risques potentiels élevés/importants), 5 % en diagnostic *in vitro*, et 1 % en classe III (risques élevés)[166] Sont compris, d'une part, des exigences générales relatives aux investigations cliniques conduites pour établir la conformité des dispositifs et la conduite des études cliniques (ce qui à notre opinion pourra concerner le testing des outils IA[167]) et, d'autre part, des enregistrements et notifications des événements indésirables survenant pendant les investigations cliniques, et donc, notamment, la détection de biais. L'évaluation clinique et la documentation y afférente font l'objet d'une mise à jour régulière[168] à l'aide des données cliniques obtenues par le fabricant (dans le cadre d'un plan à la fois de surveillance clinique (Annexe XIV) et du plan de surveillance après commercialisation visé à l'article 84.

Le Règlement distingue les différents acteurs (fabricant[169], mandataire, importateur, exportateur) de la *supply chain* du produit et distingue les obligations propres à chacun d'eux. On souligne que ce règlement n'envisage pas d'obligations propres aux utilisateurs, ainsi, les hôpitaux, les EHPAD ou les médecins utilisant des systèmes d'intelligence artificielle, qu'ils s'agissent de robots médicaux, de systèmes de diagnostic ou autres. Cette lacune qui s'explique pour nombre de dispositifs médicaux soulève un problème particulier lorsqu'il est question de système de *machine learning* où l'utilisateur professionnel contribue par les données qu'il introduit et les pratiques qui sont les siennes à construire et faire évoluer le système d'intelligence artificielle. A cet égard, on ne peut que considérer comme bienvenue l'application de la proposition de règlement général sur l'IA qui s'applique à certains dispositifs médicaux utilisant la technologie de l'IA et qualifiables de systèmes « à haut risque »[170] [171]. Ainsi, l'article 29 de la proposition de règlement AI Act que nous analyserons infra, n° 34, propose un certain nombre d'obligations à l'utilisateur professionnel qui se devra de contri-

[166] U. J. MUEHLEMATTER and *alii*, « Approval of artificial intelligence and machine learning-based medical devices in the USA and Europe (2015-20) : a comparative analysis », *Lancet Digit Health* 2021 ; 3 : e195–203, vol. 3, Issue 3, E195-E203, March 01, 2021, Open Access Published :January 18, 2021, DOI :https://doi.org/10.1016/S2589-7500(20)30292-2.

[167] Attention cependant au sur-apprentissage, ou *overfitting*. L'algorithme apprend à partir des données de test et construit ainsi un modèle qui lui permettra de généraliser ce qu'il a appris à d'autres ensembles de données mais s'il « sur-apprend », son modèle ne sera pertinent que pour les données d'entrainement

[168] Pour les dispositifs de classe III et les dispositifs implantables, le rapport d'évaluation et, s'il y a lieu, le résumé des caractéristiques de sécurité et des performances cliniques visé à l'article 32, sont mis à jour au moins annuellement en y ajoutant les données en question

[169] Le fabricant est défini comme étant "*toute personne physique ou morale qui fabrique ou remet à neuf un dispositif ou fait concevoir, fabriquer ou remettre à neuf un dispositif, et commercialise ce dispositif sous son nom ou sous sa marque*", c'est l'acteur dont les responsabilités sont les plus élevées au sens du règlement 2017/745.

[170] Sur la définition de cette notion, voir infra, n° 36.

[171] Sur ce point, les réflexions de A. KISELEVA, « AI as a medical device : Is it enough to ensure Preformace transparency and accountability ?", *European Pharmaceutical law Review*, vol. 4, 2020, en particulier, p. 8 et 9.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

buer à assurer le fonctionnement fiable et non dommageable du système et ce, dans la durée.

34. De quelques questions et lacunes à propos du Règlement : Dernière remarque à propos de ce Règlement, celui-ci a pour objectifs la protection des patients et la sécurité des dispositifs et couvrent des aspects (voir l'annexe 1 du règlement) comme :

Performance : le fabricant doit indiquer clairement les limites d'utilisation de son dispositif, le groupe de patients visé, les paramètres et leurs limitations, les contre-indications. « *If applicable, manufacturers must also include the performance characteristics, accuracy, precision and stability, the limits of accuracy and the analytical performance.*"

Minimisation des biais ("*From a legal point of view, bias is any prejudiced or partial personal or social perception of a person or group"*)

Reproductibilité, définie comme "*the degree to which the software output and performance under the same conditions produces results that can be accepted as being identical*[172]" et fiabilité : "*Reliability in this context is understood as "the ability of a system or an entity within that system to perform its required functions under stated conditions for a specific period of time"*

Sécurité *(Safety)*, définie comme "*devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, […] adopt appropriate means to reduce as far as possible consequent (A) risks or (B) impairment of performance […] in the event of a single fault condition*".

Le COCIR[173] note que la couverture de ces aspects ne permet pas de garantir au monde médical et aux patients la confiance (*Trust*) dans le fonctionnement de tels dispositifs. La nécessité de cette confiance particulièrement souhaitable dans le domaine de la santé mais en outre 'pierre de touche' de la troisième voie européenne dans sa volonté de développer les systèmes d'IA oblige à aborder d'autres aspects d'un *design* éthique des systèmes d'intelligence artificielle. Ces autres aspects concernent, d'abord la transparence et l'« explicabilité » du fonctionnement des algorithmes et ensuite la confidentialité et la protection des données exigées par le RGPD. Tant ces deux aspects non couverts par le Règlement sur les dispositifs que ceux déjà identifiés par ce Règlement sont mis en évidence par le *High Level Group of Experts on AI* mis en place par la Commission européenne[174] On sait que les conclusions de ce Groupe

[172] "*Many devices have a performance that is subject to change, e.g., a Computed Tomography (CT) machine used to visualize the same object a thousand times is subject to wear and tear and to fluctuations in environmental conditions. It will never run exactly the same, but still, when using the same acquisition parameters a user will generally consider the output identical, even across large time spans, because the machine will have been calibrated regularly to keep its performance on a minimum performance level established by the manufacturer so as to keep output identical in light of the intended purpose of the device and considering state-of-the-art.*" (COCIR, *op. cit.*, p. 22)

[173] COCIR, *op. cit.*, p. 16 et s.

[174] HLGE (High Level Group of experts on AI). Sur ce groupe et ses travaux, https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence) et notamment sa publication des *LIGNES DIRECTRICES EN MATIERE D'ETHIQUE pour UNE IA DIGNE DE CONFIANCE* (publiés le 8 avril 2019), texte disponible sur le site : Ethics guidelines for trustworthy AI – Publications Office of the EU (europa.eu) – https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

relèvent sept critères d'une construction éthique d'une application IA[175] et que leurs travaux ont directement contribué à la rédaction par la Commission européenne d'une proposition de Règlement en matière d'IA : l'« *AI Act* »[176], qui, par ailleurs, adapte la structure et l'organisation mises en place par le Règlement sur les dispositifs médicaux, cette fois dans tous les domaines des applications de l'IA : finance, emploi, éducation, police, assurance, … Ainsi, l'application combinée du règlement sur les dispositifs médicaux et de la proposition *d'AI Act* élargira les exigences éthiques relatives aux systèmes d'IA en matière médicale, en particulier aux exigences de transparence et d'*accountability*[177].

Au-delà, on s'interroge sur l'étendue de l'application du Règlement aux dispositifs d'intelligence médicale en matière de santé : le dispositif réglementaire est-il applicable en matière de dispositifs dits de 'bien-être', par exemple au bracelet dit intelligent permettant à son porteur de suivre l'évolution de ses pulsions cardiaques, l'impact calorique de son activité, etc. ? La question est d'autant plus délicate que ce dispositif peut s'intégrer dans un suivi médical. L'autre difficulté est due à l'évolution permanente du logiciel d'intelligence artificielle qui permet difficilement d'appréhender les risques liés à son utilisation alors que la directive se centre sur des dispositifs relativement figés. Ainsi, l'exosquelette prévu initialement comme technologie de réparation d'un membre déficient ou amputé se voit ouvrir de nouvelles finalités lorsqu'il s'agit de permettre à une personne d'améliorer ses performances. L'évaluation réclamée par la réglementation européenne doit-elle tenir compte de cette évolution de finalité[178] ?

6 Les propositions de règlements sur l'IA et sur les robots

35. L'« *AI Act* » et le design éthique – Le 21 avril 2021, la Commission publiait sa proposition de règlement « instaurant des règles harmonisées en matière d'intelligence artificielle », en abrégé l'« *Artificial Intelligence Act* »[179]. Il s'agit bien, affirme Mme VESTAGER lors de la présentation de la proposition, de mettre en œuvre par ce

[175] Les sept critères dégagés par les guidelines sont respectivement : Human Agency and Oversight ; Technical Robustness and Safety ; Privacy and Data Governance ; Transparency ; Diversity, Non-discrimination and Fairness ; Societal and Environmental Well-being ; Accountability. Sur les méthodes d'évaluation et les critères à prendre en compte, voir le site de présentation d'Altai (Assessment List fot Trustworthy AI) : https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence

[176] Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL ÉTABLISSANT DES RÈGLES HARMONISÉES CONCERNANT L'INTELLIGENCE ARTIFICIELLE (LÉGISLATION SUR L'INTELLIGENCE ARTIFICIELLE) ET MODIFIANT CERTAINS ACTES LÉGISLATIFS DE L'UNION COM(2021), Bruxelles 21 avril 2021, 206 final SEC(2021) 167 final – SWD(2021) 84 final – SWD(2021) 85 final.

[177] Sur ce point, lire A. KISELEVA, « AI as a medical device : between the Medical Devices Framework and the General AI Regulation », in *Time to reshape the Digital Society,* 40th anniversary of the CRIDS (sous la direction de H. Jacquemin), Larcier, Cahier du CRIDS, n° 52, 2022, p. 495 et s.

[178] La question est posée dans le rapport du COCIR (EU Coordination Committee for Radiological, Electromedical and Healthcare IT Industry), *AI in EU medical Device Legislation*, Sept. 2020, p. 11. Rapport disponible sur le site du COCIR https://www.cocir.org/media-centre/publications/article/cocir-analysis-on-ai-in-medical-device-legislation-september-2020.html

[179] Pour une critique développée de la proposition, lire l'excellent rapport de N.SMUHA, E.AHMED-RENGERS, A HERKENS et alii, « How the EU can achieve Legally Trustworthy AI : A response to the European Commission's proposal for an Artificial intelligence Act », *University of Birmingham Leads Lab report*, disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991. Le texte est en discussion en première lecture au Parlement où la question de savoir quelle commission parlementaire assumera le rôle de leader (IMCO ?) est toujours pendante et au Conseil qui, sous présidence slovène, espère avoir terminé une première lecture pour le mois de décembre.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

texte les principes mêmes d'excellence et de confiance : « *En matière d'intelligence artificielle, la confiance n'est pas un luxe mais une nécessité absolue. En adoptant ces règles qui feront date, l'UE prend l'initiative d'élaborer de nouvelles normes mondiales qui garantiront que l'IA soit digne de confiance. En établissant les normes, nous pouvons ouvrir la voie à une technologie éthique dans le monde entier, tout en préservant la compétitivité de l'UE. À l'épreuve du temps et propices à l'innovation, nos règles s'appliqueront lorsque c'est strictement nécessaire : quand la sécurité et les droits fondamentaux des citoyens de l'Union sont en jeu.* ». Le but du texte est quadruple : "

veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés soient sûrs et respectent la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union ;

garantir la sécurité juridique pour faciliter les investissements et l'innovation dans le domaine de l'IA ;

renforcer la gouvernance et l'application effective de la législation existante en matière de droits fondamentaux et des exigences de sécurité applicables aux systèmes d'IA ;

faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et dignes de confiance, et empêcher la fragmentation du marché. »

La proposition de règlement se réfère aux législations sectorielles qui peuvent déjà exister[180]. Elle se propose comme un cadre général de réglementation de l'IA et son adoption nécessitera sans doute des adaptations à la marge du Règlement sur les dispositifs médicaux. Sans entrer dans le détail de la Proposition de la Commission soumise au double examen des parlementaires et du Conseil des Ministres, notons qu'elle cherche à établir un compromis entre les exigences légales et éthiques, traduisant les valeurs de l'Union et la nécessité de ne pas contraindre de manière exagérée le développement et l'initiative technologiques voire de la promouvoir[181]. Pour ce faire, le texte adopte une approche règlementaire strictement proportionnée et évolutive.

36. Une catégorisation des systèmes d'IA fondées sur les risques et les obligations liées – Il reprend l'approche fondée sur les risques qui caractérisait déjà le Règlement sur les dispositifs médicaux. Pour ce faire, la proposition énonce l'interdiction de pratiques illégales de l'intelligence artificielle[182] (art. 5) ; elle met en place un système de

[180] Notamment, des législations en matière de crédit. On note par ailleurs, l'affirmation suivante (Proposition de règlement, in Contexte de la proposition) : « *S'agissant en particulier des systèmes d'IA à haut risque liés aux produits couverts par les actes du nouveau cadre législatif (les machines, les dispositifs médicaux* (nous soulignons_) et les jouets, par exemple), les exigences applicables aux systèmes d'IA définies dans la présente proposition feront l'objet d'une vérification dans le cadre des procédures existantes d'évaluation de la conformité prévues dans les actes appropriés du nouveau cadre législatif_. »

[181] Les articles 53 et s. prévoient diverses mesures de soutien à l'innovation, en particulier le développement de certains outils d'IA dans le cadre de 'bacs à sable réglementaires' : « *Les bacs à sable réglementaires de l'IA créés par une ou plusieurs autorités compétentes des États membres ou par le Contrôleur européen de la protection des données offrent un environnement contrôlé qui facilite le développement, la mise à l'essai et la validation de systèmes d'IA innovants pendant une durée limitée avant leur mise sur le marché ou leur mise en service conformément à un plan spécifique. Cela se fait sous la surveillance et le contrôle directs des autorités compétentes afin de garantir le respect des exigences du présent règlement et, le cas échéant, d'autres dispositions législatives de l'Union et des États membres contrôlées au sein du bac à sable.* »

[182] Ainsi, les systèmes de manipulation par messages subliminaux, l'exploitation des vulnérabilités, l'utilisation par le secteur public de systèmes de « *social ranking* » entraînant de potentielles discriminations

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

contrôle et de gestion des systèmes d'IA à haut risque (art.6.2) listées dans une annexe susceptible de modification par la Commission ; elle soumet à des obligations spécifiques de transparence pour certaines applications cachées _« en particulier lorsque des dialogueurs ou des trucages vidéo ultra-réalistes sont utilisés ».__et, enfin, abandonne à l'autoréglementation du marché les autres applications présentant un risque minime.

En ce qui concerne la première catégorie, celle des risques inacceptables « *en raison de leur caractère contraire aux valeurs de l'Union européenne* », l'article 5 les liste parfois avec un manque de précision et surtout sans souci de l'évolutivité nécessaire de cette liste. Sans les citer tous, on relève les interdictions suivantes qui pourraient trouver application dans le secteur de la santé[183] :

- « *les systèmes d'IA qui exploitent les éventuelles vulnérabilités dues à l'âge ou au handicap physique ou mental d'un groupe de personnes donné*[184] *pour altérer substantiellement le comportement d'un membre de ce groupe d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers* »

- « *l'utilisation par les pouvoirs publics*[185] *ou pour leur compte, de systèmes d'IA destinés à évaluer ou à établir un classement de la fiabilité de personnes physiques au cours d'une période donnée en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues ou prédites* », dans la mesure où ce *scoring* conduit à un traitement préjudiciable injustifié ou sur base de données utilisées de manière incompatible avec les finalités de la collecte et du traitement originaire[186] ;

.

entre personnes ou groupes, de systèmes biométriques fonctionnant en temps réel et à distance, placés dans des endroits publics (par exemple, des systèmes de reconnaissance faciale, …)

[183] Selon l'opinion de l'EDPB (*European Data Protection Board*) et de l'EDPS (*European Data Protection Supervisor*), cette liste aurait dû être élargie à tous les systèmes d'évaluation sociale et à nombre de traitements de données biométriques. "*Remote biometric identification of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals' private lives, with severe effects on the populations' expectation of being anonymous in public spaces. For these reasons, the EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces – such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals – in any context. A ban is equally recommended on AI systems categorizing individuals from biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination under Article 21 of the Charter. Furthermore, the EDPB and the EDPS consider that the use of AI to infer emotions of natural persons is highly undesirable and should be prohibited.*" (EDPB/EDPS, Joint opinion (/2021 on the proposal for a regulation laying down harmonized rules on Artificial intelligence, 18 juin 2021)

[184] A noter que l'interdiction vise ici un risque collectif propre à un groupe de personnes. Par ailleurs, on s'interroge sur la raison de limiter l'interdiction aux seules IA exploitant les handicaps physiques et mentaux et de subordonner l'interdiction à la nécessité d'un dommage physique ou psychologique prévisible, l'interdiction proposée. Ne peut-on considérer que certains *nudges* exploitant la vulnérabilité de certains groupes en dehors de ceux cités ne devraient pas être également considérés ? A cet égard, le Projet de Recommandation CM/Rec(2021) du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage du Comité consultatif de la Convention n° 108, article 1.j.) : « *L'expression « traitements de profilage à risque élevé » peut notamment désigner … : ii. le profilage qui en raison du public visé, du contexte, de la finalité du traitement en particulier dans une situation de déséquilibre dans le pouvoir d'information, comporte un risque d'affecter ou d'influencer indûment des personnes concernées notamment lorsqu'il s'agit de mineurs ou de personnes vulnérables ; … »*

[185] … et non par les pouvoirs privés, ainsi une banque qui évaluerait le potentiel de crédit des clients. Notons que nombre de systèmes privés de *social rating* seront considérés comme des systèmes à haut risque.

[186] On retrouve là des principes du RGPD : non utilisation à des fins illégitimes ou incompatibles.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

Les articles 52 et s. soumettent à des obligations particulières de transparence certains systèmes utilisant l'IA. Parmi les applications intéressant notre propos, on relève l'obligation d'informer les personnes interagissant avec un système d'IA de la présence d'un robot comme interlocuteur. Même obligation d'information des personnes concernées en cas d'utilisation de systèmes de reconnaissance d'émotions ou de profilage sur base de données biométriques.

La dernière catégorie réglementée concerne les applications IA dites à haut risque. L'article 6.1 (a) renvoie à certaines catégories de dispositifs médicaux, dans la mesure où l'annexe 2 mentionne explicitement le règlement sur les dispositifs médicaux[187] : *« Un système d'IA mis sur le marché ou mis en service, qu'il soit ou non indépendant des produits visés aux points a) et b), est considéré comme à haut risque lorsque les deux conditions suivantes sont remplies :*

(a) le système d'IA est destiné à être utilisé comme composant de sécurité d'un produit couvert par les actes législatifs d'harmonisation de l'Union énumérés à l'annexe II, ou constitue lui-même un tel produit ;

(b) le produit dont le composant de sécurité est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une évaluation de la conformité par un tiers en vue de la mise sur le marché ou de la mise en service de ce produit conformément aux actes législatifs d'harmonisation de l'Union énumérés à l'annexe II.

Outre cette application de la notion de systèmes à haut risque aux dispositifs médicaux, l'annexe III énumère huit catégories de systèmes à haut risque dont peu concernent la santé. On souligne cependant la prise en compte dans la liste, les systèmes biométriques d'identification (reconnaissance faciale ; utilisation des empreintes digitales, etc.), les applications en ce qui concerne l'accès ou la jouissance de services publics (en particulier les systèmes d'assistance médicale ou d'urgence sanitaire) ou de services privés essentiels (prioritisation de l'accès à des systèmes de santé ou de secours).

37. Les obligations des fournisseurs et des autres acteurs de la *supply chain* - Les fournisseurs (*providers)* de systèmes IA à haut risque[188] se voient imposer de multiples devoirs (art .16)[189]. La proposition impose, pour les systèmes dits à haut-risque, un

[187] Pour rappel, sont repris dans le règlement sur les dispositifs médicaux comme systèmes est soumise à une évaluation de conformité : « La classification des dispositifs médicaux en fonction des risques « santé et sécurité » liés à leur fonctionnement : (article 51) -« *Tous les dispositifs actifs destinés à commander, à contrôler ou à agir directement sur les performances des dispositifs implantables actifs relèvent de la classeIII* » et, plus loin, que « *les logiciels destinés à fournir des informations utilisées pour prendre des décisions à des fins thérapeutiques ou diagnostiques relèvent de la classeIIa, Les logiciels destinés à contrôler des processus physiologiques relèvent de la classeIIa, sauf s'ils sont destinés à contrôler des paramètres physiologiques vitaux, lorsque des variations de certains de ces paramètres peuvent présenter un danger immédiat pour la vie du patient, auxquels cas ils relèvent de la classe IIb.* »

[188] Soit selon la définition de la proposition (article 1. (2) : « « *fournisseur* », *une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit* ». L'utilisation des mots 'mise sur le marché' exclut-elle les autorités publiques et les institutions universitaires ?

[189] Art. 16 du projet de règlement *: « Les fournisseurs de systèmes d'IA à haut risque :*
(a) veillent à ce que leurs systèmes d'IA à haut risque soient conformes aux exigences énoncées au chapitre 2 du présent titre ;
(b) mettent en place un système de gestion de la qualité conforme à l'article 17 ;
(c) établissent la documentation technique du système d'IA à haut risque ;

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

système de gestion des risques (art. 9) qui implique le suivi de bonnes pratiques en matière d'évaluation des systèmes (absence de biais, qualité des données, …). L'article 10 mentionne divers devoirs liés à la gouvernance des données, ainsi le *testing* et la validation des choix de *design* et des données prises en compte, l'examen des biais possibles, etc. On ajoute les obligations de documentation technique, détaillée, par ailleurs, dans son contenu et son format par l'annexe IV de la proposition (art.11 et 18), de *loggings* (art. 12[190] et 20) et surtout de surveillance humaine (*human oversight)*[191]. Le projet mentionne le devoir de coopération avec les autorités nationales compétentes y compris en fournissant l'accès à tous les logs. En particulier, l'article 19 mentionne l'obligation d'une évaluation préventive interne au fournisseur, qui doit assurer la conformité du système aux exigences du Règlement et l'apposition d'un certificat européen de conformité avant toute mise sur le marché[192].

D'autres obligations concernent d'autres acteurs : à côté des fournisseurs de systèmes à haut risque, la proposition identifie les producteurs, les distributeurs, les importateurs, les utilisateurs ayant recours à un système à haut risque dans le cadre de leurs activités professionnelles (ainsi un praticien de l'art de guérir acquérant un robot chirurgical ou un hôpital ayant recours dans un service à un système IA permettant de diagnostiquer la maladie de Parkinson) et ce suivant leur rôle précis lors des diverses étapes qui mènent de la conception à l'exploitation du système IA. Ce point est important dans la mesure où à la différence du RGPD (voir déjà, nos réflexions, *supra,* n° 17), concentré sur les seuls acteurs – responsable de traitement et sous-traitants, d'une part, et personnes concernées, d'autre part –, la proposition de Règlement prend en compte la diversité des acteurs qui constituent la chaîne d'intervenants, depuis la conception du système d'intelligence artificielle jusqu'à son suivi, même si la qualification de certains

(d) assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque, dans la mesure où ces journaux se trouvent sous leur contrôle ;
(e) veillent à ce que le système d'IA à haut risque soit soumis à la procédure d'évaluation de la conformité applicable, avant sa mise sur le marché ou sa mise en service ;
(f) respectent les obligations en matière d'enregistrement prévues à l'article 51 ;
(g) prennent les mesures correctives nécessaires si le système d'IA à haut risque n'est pas conforme aux exigences énoncées au chapitre 2 du présent titre ;
(h) informent les autorités nationales compétentes des États membres dans lesquels ils ont mis le système d'IA à disposition ou en service et, le cas échéant, l'organisme notifié, de la non-conformité et de toute mesure corrective prise ;
(i) apposent le marquage CE sur leurs systèmes d'IA à haut risque afin d'indiquer la conformité au présent règlement, conformément à l'article 49 ;
(j) à la demande d'une autorité nationale compétente, apportent la preuve de la conformité du système d'IA à haut risque aux exigences énoncées au chapitre 2 du présent titre.

[190] Article 12 : « *1. La conception et le développement des systèmes d'IA à haut risque prévoient des fonctionnalités permettant l'enregistrement automatique des événements (« journaux ») pendant le fonctionnement de ces systèmes. Ces fonctionnalités d'enregistrement sont conformes à des normes ou à des spécifications communes reconnues ; 2. Les fonctionnalités d'enregistrement garantissent un degré de traçabilité du fonctionnement du système d'IA tout au long de son cycle de vie qui soit adapté à la destination du système.* »

[191] Art. 14.1 : « La conception et le développement des systèmes d'IA à haut risque permettent, notamment au moyen d'interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant la période d'utilisation du système d'IA. ». On notera le flou d'une telle disposition.

[192] Les annexes Vi et VII définissent la procédure soit légère et purement interne si le fournisseur (*provider*) s'appuie sur des systèmes se référant à des standards harmonisés, soit plus lourde et dans ce cas externe auprès d'un organe de notification (autorité de contrôle) si tel n'est pas le cas. Cette évaluation est interne au fournisseur, ce qui peut faire craindre un certain laxisme dans l'interprétation des exigences du futur règlement, sous réserve certes du contrôle par l'autorité nationale de supervision évoquée dans le paragraphe suivant. On ajoute que l'absence d'évaluation ou de certificat ou leur mauvaise réalisation sont lourdement sanctionnées.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

intervenants risque de poser difficulté[193]. En particulier, comme déjà noté supra n° 30, elle corrige le règlement sur les dispositifs médicaux en insistant sur les obligations des utilisateurs des systèmes d'intelligence artificielle, bien souvent appelés à participer aux tests, à fournir les données voire par leur pratique à influer sur le fonctionnement du système. Ainsi, l'article 29[194] de la proposition oblige l'utilisateur à suivre les recommandations du « fournisseur », à l'alerter au cas où des risques surviendraient, de veiller à une évaluation du système tel qu'utilisé.

38. La création d'autorités de contrôle – Enfin, toujours sur le modèle du Règlement « Dispositifs médicaux », l'article 30 oblige les Etats membres à créer une autorité dite de notification (*notifying body)*," Chaque État membre désigne ou établit une autorité « *chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle* ». On note que coiffent ces autorités de notification, des autorités de supervision, « *établies ou désignées par chaque État membre aux fins d'assurer l'application et la mise en œuvre du présent règlement y compris le pouvoir de sanctionner le non-respect des prescrits. Les autorités nationales compétentes sont organisées de manière à garantir l'objectivité et l'impartialité de leurs activités et de leurs tâches* ». C'est à propos de ces autorités de supervision que l'EDPB, dans son avis commun avec l'EDPS[195], souhaitait que leurs tâches soient confiées aux autorités de protection des données : « *The designation of data protection authorities (DPAs) as the national supervisory authorities would ensure a more harmonized regulatory approach, and contribute to the consistent interpretation of data processing provisions and avoid contradictions in its enforcement among Member States. Consequently, the EDPB*

[193] La notion de fournisseur est définie par l'article 3 point (2) comme suit : *« fournisseur », une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit ; » ;* celle d'utilisateur au point (4) *: « utilisateur », toute personne physique ou morale, autorité publique, agence ou autre organisme utilisant sous sa propre autorité un système d'IA,.* ». Considérera-t-on que la banque qui achète « clé sur porte » à une entreprise spécialisée en IA est fournisseur ou utilisateur ? Quid d'une administration ou d'un hôpital, qui « outsourcent » la gestion de 'leur' système IA ? Par ailleurs, il n'est pas fait mention des fournisseurs des éléments du système : par exemple une base de données ou un algorithme

[194] *« 1. Les utilisateurs de systèmes d'IA à haut risque utilisent ces systèmes conformément aux notices d'utilisation accompagnant les systèmes, conformément aux paragraphes 2 et 5.*
2. Les obligations énoncées au paragraphe 1 sont sans préjudice des autres obligations de l'utilisateur prévues par le droit de l'Union ou le droit national et de la faculté de l'utilisateur d'organiser ses propres ressources et activités aux fins de la mise en œuvre des mesures de contrôle humain indiquées par le fournisseur.
3. Sans préjudice du paragraphe 1, pour autant que l'utilisateur exerce un contrôle sur les données d'entrée, il veille à ce que ces dernières soient pertinentes au regard de la destination du système d'IA à haut risque.
4. Les utilisateurs surveillent le fonctionnement du système d'IA à haut risque sur la base de la notice d'utilisation. Lorsqu'ils ont des raisons de considérer que l'utilisation conformément à la notice d'utilisation peut avoir pour effet que le système d'IA présente un risque …, ils en informent le fournisseur ou le distributeur et suspendent l'utilisation du système. Ils informent également le fournisseur ou le distributeur lorsqu'ils constatent un incident grave ou un dysfonctionnement … et ils interrompent l'utilisation du système d'IA ….
6. Les utilisateurs de systèmes d'IA à haut risque assurent la tenue des journaux générés automatiquement par ce système d'IA à haut risque, dans la mesure où ces journaux se trouvent sous leur contrôle. Les journaux sont conservés pendant une période appropriée au regard de la destination du système d'IA à haut risque et des obligations légales applicables en vertu du droit de l'Union ou du droit national.
7. Les utilisateurs de systèmes d'IA à haut risque utilisent les informations fournies en application de l'article 13 pour se conformer à leur obligation de procéder à une analyse d'impact relative à la protection des données en vertu de l'article 35 du règlement (UE) 2016/679 (Ndla : le RGPD) ou de l'article 27 de la directive (UE) 2016/680, le cas échéant. »

[195] Opinion déjà citée (note 52)

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

and the EDPS consider that data protection authorities should be designated as national supervisory authorities pursuant to Article 59 of the Proposal." Cette position peut s'expliquer si on se limite à la considération des seuls risques d'atteinte à nos libertés individuelles. Elle s'avère plus critiquable si on considère également les autres risques collectifs et sociétaux liés aux applications de l'intelligence artificielle.

Cette dernière considération sur l'élargissement des enjeux à prendre en considération dans l'examen des applications IA conduit à la nécessité, en particulier dans le domaine de la santé de rappeler, au nom du principe de précaution[196], la nécessité d'une évaluation publique ouverte à toutes les parties intéressées de certaines technologies dont l'impact sur notre fonctionnement d'humain, sur nos libertés individuelles mais au-delà sur la justice sociale et les risques de discrimination de certains groupes est important. Cela nécessite de créer des espaces et des temps de réflexion dans les calendriers des projets, également de pouvoir arrêter la chaîne de production en cas de problème. Ce souhait n'est pas évident à voir réaliser dans des environnements d'« entreprises » ou d'administrations en charge de la santé soucieuses de rentabilité et craignant la concurrence. La difficulté vient également du fait que cette réflexion ne sera utile et possible que par une équipe pluridisciplinaire créée au sein de l'entreprise ou appelée à assister l'entreprise dans ce parcours réflexif. Cette exigence de pluridisciplinarité et de représentation des différents '*stakeholders'* dans l'évaluation éthique, en particulier des systèmes d'intelligence artificielle est réclamée. On la retrouve dans la plupart des textes internationaux d'éthique[197].

39. Et les robots ? – Une autre proposition de règlement dit « Machines et Equipements »[198], publiée le même jour que celle dite « *AI Act* » par la Commission, remplacerait la directive de 2006 « machines », qui définissait des exigences en matière de santé et de sécurité dans le secteur des machines. La proposition garantit que les machines de nouvelle génération intégrant des logiciels en particulier d'IA comme, par exemple, les robots aide-soignant ou ceux chirurgicaux, offrent, au regard des nou-

[196]Le point 2.5. de la Recommandation du Conseil de l'Europe en matière de mégadonnées définit comme suit la signification du principe de précaution_ : « Les responsables du traitement devraient procéder à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées afin 1) d'identifier et d'évaluer les risques de chaque activité de traitement de mégadonnées et de ses incidences potentiellement négatives sur les droits et libertés fondamentales des personnes, en particulier le droit à la protection des données à caractère personnel et le droit à la non-discrimination, en tenant compte des impacts sociaux et éthiques ; 2) de mettre au point et de prévoir des mesures appropriées, notamment dès la conception (by-design) et par défaut (by default), pour atténuer les risques qui seront identifiés ; 3) de suivre de près l'adoption et l'efficacité des solutions proposées._ ».

[197]Le point 2.6 de la recommandation du Conseil de l'Europe à propos des mégadonnées note : « *Le processus d'évaluation devrait être mené par des personnes dotées des qualifications professionnelles et des connaissances adéquates pour apprécier les différents impacts, y compris dans leurs dimensions juridique, sociale, éthique et technique.* » et le point 2.7 précise. :« *En ce qui concerne l'utilisation de mégadonnées, susceptible de porter atteinte aux droits fondamentaux, les Parties devraient encourager la participation des différents acteurs (par exemple, des personnes ou groupes qui pourraient être concernés par l'utilisation des mégadonnées) au processus d'évaluation des risques et à la conception du traitement des données.* » et le point 2.7 précise. :« *En ce qui concerne l'utilisation de mégadonnées, susceptible de porter atteinte aux droits fondamentaux, les Parties devraient encourager la participation des différents acteurs (par exemple, des personnes ou groupes qui pourraient être concernés par l'utilisation des mégadonnées) au processus d'évaluation des risques et à la conception du traitement des données.* ». Pour une comparaison entre les documents relatifs à l'éthique de l'IA émis par quatre organisations publiques internationales (OCDE, UNESCO, Conseil de l'Europe, Union européenne, lire Y. POULLET, « « About some international documents relating to the ethics of artificial Intelligence », in *Time to reshape the Digital Society,* 40th Anniversary of the CRIDS (sous la direction de H. Jacquemin), Larcier, 2021, p. 523 – 541

[198]Proposal for a regulation of the European Parliament and of the Council on machinery products, Brussels, 21.4.2021 COM(2021) 202 final 2021/0105 (COD)

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

veaux risques créés[199], toute la sécurité requise aux utilisateurs et aux consommateurs et encouragera l'innovation. Alors que le règlement sur l'IA traitera des risques liés à la sécurité que présentent les systèmes d'IA, le nouveau règlement sur les machines garantira une intégration sûre des systèmes d'IA dans les machines et les responsabilités liées au fonctionnement de ces produits d'intégration[200]. En particulier, le règlement exige pour les machines et équipements à haut risque définis à l'annexe du règlement, de suivre une procédure d'évaluation de conformité. Les critères d'appréciation des risques sont fixés dans le texte du règlement (art. 5). Le texte (art. 6 et s.) impose aux producteurs, importateurs, distributeurs une série d'obligations en matière de documentation, de tests, etc. Enfin, la proposition impose (art. 24 et s.) aux États membres de désigner un organe de notification qui peut s'appuyer ou non sur un organe externe d'accréditation[201]. On ajoute qu'en cas de défaillance d'un produit ou de crainte raisonnablement suffisante de non-respect par un produit des requis en matière de sécurité ou de santé, l'autorité de surveillance peut exiger des mesures correctives (art. 36.3 et 41.1).

CONCLUSIONS

40. Une relation humaine à protéger – Il est certain que les techniques d'intelligence artificielle bouleverseront les pratiques des acteurs de la santé. Ainsi, cette interposition de l'objet technologique heurte le principe même de la relation soignant-professionnel de santé. *En effet, « la relation soignant/patient est au cœur même du soin. S'il est largement admis par tous que l'IA peut faire gagner en efficacité, en précision et en rapidité pour des actes techniques, déléguer à une machine le rôle relationnel du soignant peut apparaître bien plus choquant. C'est dans ce relationnel que s'établit la relation de confiance, gage de qualité des soins. Confier cet aspect à un robot peut certes présenter des avantages, dans un contexte de pénurie de personnel et/ou de rationalisation des coûts, mais risque aussi de faire perdre un élément essentiel de la prise en charge : le colloque singulier, l'empathie, conduisant à une déshumanisation de la relation. »*[202]. Au-delà, il est souligné que la médiation de la relation par un outil technologique conduit ou risque de conduire à déresponsabiliser le professionnel de la santé[203], sans que, pour autant, la responsabilité du dispositif lui-même puisse toujours être mise en cause. On ajoute que dans le domaine de la santé, le fonction-

[199] Voir l'*Explanatory Memorandum,* n° 11, p. 16.

[200] Sur ce point, la proposition s'appuie sur l'excellent rapport de la Commission au Parlement européen, au Conseil et au Comité économique et social européen, Rapport du 19 février 2020 sur les conséquences de l'intelligence artificielle, de l'Internet des objets et de la robotique sur la sécurité et la responsabilité, COM/2020/64 final, *disponible à l'adresse* https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implicationsai-Internet-things-and-robotics-0_en. et la Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle (2020/2014(INL))

[201] Article 25.3.

[202] Sur ce point et de nombreuses références, lire mes réflexions in « Construire un cadre juridique pour l'e-Health, in *La protection des données médicales,* J. HERVEG (éd.), LGDJ, 2009, p. 119 et s. : « *En d'autres termes, le partage du dossier n'est pas défini a priori en fonction des nécessités de la continuité des soins, mais a priori comme une possibilité qui facilitera la continuité des soins, sans qu'il soit nécessaire de connaître les intervenants nécessaires à celle-ci et sans que ce soit le médecin à la base de la chaîne des soins qui puisse fixer ceux qui participent à une telle continuité.* »

[203] Sur ce point, les réflexions très pertinentes de N. NEVEJANS, « L'influence des logiciels d'aide à la décision sur le processus décisionnel médical à la lumière du droit et de l'éthique », in *Innovations en santé publique, des données personnelles aux données massives (Big data*), sous la direction de C. HERVE et M. STANTON-JEAN, Dalloz, 2018, p. 113 à 123.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

nement des applications d'IA dans la mesure où ces dernières fondent leurs décisions ou du moins leurs résultats sur des corrélations qui, par la vertu du *deep learning*, s'éloignent de plus en plus du schéma cognitif de départ, heurte le traditionnel raisonnement médical. Comme le note le CNOM, l'intelligence artificielle « *constitue une révolution assez importante puisque la médecine s'attache traditionnellement à la recherche des causes de la maladie et c'est le but de la médecine. Or, on s'aperçoit avec le big data qu'on arrive à établir des corrélations mais qu'on ne peut pas expliquer. On se demande finalement quelle est l'utilité d'expliquer certaines corrélations.* »[204]

Il est patent que si l'Etat veut permettre le développement d'une intelligence artificielle au service des citoyens et non de l'industrie qui développe moult produits et applications en la matière, il se doit d'abord d'élargir les catégories de professionnels de santé au regard du rôle joué par de nouveaux acteurs dans la chaîne des soins ou de la recherche médicale et assigner à ces acteurs une responsabilité dans la conception, l'élaboration et le suivi des outils d'IA. Il se doit également de veiller à revoir de manière profonde la formation des professionnels de santé[205] en incluant dans les programmes tant une formation à l'éthique à la sécurité, aux aspects juridiques à prendre en compte lors de l'utilisation de telles technologies (en particulier, les règles relatives à la responsabilité, au secret professionnel et à la *privacy*)[206].

41. Des balises légales à l'utilisation de robots et de systèmes d'IA – Dans le domaine médical, le recours à l'IA et aux robots intelligents[207]. *" Member States should ensure that human-robot interactions comply with the same values and principles that apply to any other AI systems, including human rights and fundamental freedoms, the promotion of diversity, and the protection of vulnerable people or people in vulnerable situations"* ; doit suivre des règles simples, comme le rappelle le projet de recommen-

[204] Voir sur ce point, le débat organisé par la CNOM suite au Livre Blanc, *débats Médecine du futur*,20.02.2018, p. 8, disponible à l'adresse : https://www.conseil-national.medecin.fr/node/2602.

[205] Sur la nécessité de revoir la formation des professionnels de la santé, lire entre autres, le rapport VILLANI (Rapport déjà cité, p. 198 et s.) et les réflexions du CNOM dans le Livre Blanc (p. 29 et s.) : « *Comme le CNOM, la Conférence des doyens de médecine a en effet identifié la « transformation des modalités d'apprentissage dans une société connectée où l'information est abondante » comme l'un des enjeux décisifs des années à venir* »

[206] Ainsi, reprenant la recommandation de la CNOM (CNOM, *Livre Blanc* déjà cité, Recommandation n° 24), il s'impose de rappeler les principes éthiques « *de bienveillance, de non-maltraitance, d'autonomie de la personne et de justice appliqués au monde de la santé et du soin. (Ces principes) doivent toujours, et peut-être même plus que jamais, être présents à l'esprit. Et cela quand bien même les conditions, les moyens, les circonstances, la société dans lesquels ils s'appliquent se trouveraient bouleversés par la révolution numérique en marche. L'humanisme dans la relation du médecin et du patient peut se trouver renforcé par les technologies dont nous parlons. En effet, l'humanisme médical serait une pure apparence de bienveillance s'il ne se fondait que sur de bons sentiments. Il doit s'établir tout autant sur la compétence du médecin c'est-à-dire sur les connaissances scientifiques renforcées qui peuvent émerger du traitement des grandes masses de données, que sur la capacité du médecin à être à l'écoute des inquiétudes de la personne appréhendant la maladie dont elle est atteinte tant sur le plan physique que psychologique. Cette personne malade acquiert d'ailleurs elle-même, de plus en plus souvent, une connaissance profane, mais vécue, de sa maladie en la partageant dans le monde associatif et numérique, et avec ses médecins et l'équipe de soins.* »

[207] Voir à ce propos les paragraphes 125 et 126 relatifs aux robots dans le domaine de la santé : " Member States should develop guidelines for human-robot interactions and their impact on human-human relationships, based on research and directed at the future development of robots, and with special attention to the mental and physical health of human beings. Particular attention should be given to the use of robots in health care and the care for older persons and persons with disabilities, in education, and robots for use by children, toy robots, chatbots, and companion robots for children and adults. Furthermore, assistance of AI technologies should be applied to increase the safety and ergonomic use of robots, including in a human-robot working environment. A special attention should be paid to the possibility of using AI to manipulate and abuse human cognitive biases "

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

dation de l'UNESCO sur l'éthique de l'IA (26) : « *The choice to use AI systems and which AI method to use should be justified in the following ways : (a) The AI method chosen should be appropriate and proportional to achieve a given legitimate aim ; (b) The AI method chosen should not infringe upon the foundational values …, in particular, its use must not violate or abuse human rights ; (c) The AI method should be appropriate to the context and should be based on rigorous scientific foundations*". Ce texte (paragraphe 123), comme d'autres, met en évidence l'importance d'une évaluation inclusive (ouverte à toutes les catégories d'intérêts affectés par l'utilisation d'un système d'IA) et multidisciplinaire, capable d'éviter les biais et erreurs et de respecter les libertés des patients et les nécessités de transparence[208].

En outre, on note l'absolue nécessité d'appliquer le principe de précaution[209], en particulier dans les applications IA médicales ou de bien-être dont la finalité est en particulier, soit la prédiction de notre santé grâce en particulier aux données génétiques ou aux données neurologiques, soit l'augmentation des performances humaines, qu'à cet égard les questions de libertés individuelles, de dignité et de justice sociale doivent être examinées soigneusement et qu'un débat public permettant l'évaluation de certaines de ces technologies dont l'enjeu est particulièrement significatif et implique des choix de société, doit être organisé, si possible avec l'ensemble des acteurs y compris les patients. Le cas échéant, il sera utile que les pouvoirs publics édictent des recommandations voire des législations relatives à des applications particulièrement sensibles[210]. Ce rappel du principe de précaution ne s'oppose pas à l'approche 'bac à

[208] *« Member States should pay particular attention in regulating prediction, detection and treatment solutions for health care in AI applications by :*
(a) ensuring oversight to minimize and mitigate bias ;
(b) ensuring that the professional, the patient, caregiver or service user is included as a "domain expert" in the team in all relevant steps when developing the algorithms ;
(c) paying due attention to privacy because of the potential need of being medically monitored and ensuring that all relevant national and international data protection requirements are met ;
(d) ensuring effective mechanisms so that those whose personal data is being analysed are aware of and provide informed consent to the use and analysis of their data, without preventing access to health care ;
(e) ensuring the human care and final decision of diagnosis and treatment are taken always by humans while acknowledging that AI systems can also assist in their work ; and
(f) ensuring, where necessary, the review of AI systems by an ethical research committee prior to clinical use."

[209] Ou, selon l'expression de J.P. COBBAUT, une « éthique de la vigilance ». Le principe de précaution a été reconnu en droit international public par la déclaration de Rio (Juin 1992) en son principe 15 qui affirme : "'*In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation "(« En cas de risque de dommages graves ou irréversibles, l'absence de certitude scientifique absolue ne doit pas servir de prétexte pour remettre à plus tard l'adoption de mesures effectives visant à prévenir la dégradation de l'environnement. »)*. En droit communautaire, ce principe reconnu en droit de l'environnement sensu stricto a été élargi à d'autres domaines : « *La Cour rappelle l'importance du principe de précaution (consacré pour la première fois par la Déclaration de Rio), qui 'a vocation à s'appliquer en vue d'assurer un niveau de protection élevée de la santé, de la sécurité des consommateurs et de l'environnement, dans l'ensemble des activités de la Communauté* » (G. C. Rodríguez Iglesias *et al.*, *National Farmers Union,* Cour de Justice de l'Union européenne 1998). Pour une application en matière de protection des données, L. COSTA, "Privacy and the precautionary principle", *Computer Law & Security Review*, 2011, p. 14 à 24

[210] A ce propos, on citera : dans le domaine des applications IA dans le domaine des neurotechnologies, la *Recommandation de l'OCDE sur l'innovation responsable dans le domaine des neurotechnologies*, adopté par le Conseil de l'OCDE, le 11 décembre 2019 (OECD/legal/0457) : « La recommandation a vocation à fournir des orientations pour chaque étape du processus d'innovation- la recherche, le transfert de technologie, l'investissement, la commercialisation, la réglementation, etc.- de manière à maximiser les avantages tout en minimisant les risques. Elle met l'accent sur l'importance (1) de valeurs fondamentales telles que la gestion responsable, la confiance et la sécurité et le respect de la vie privée dans ce contexte

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

sable'[211] qui permet de suivre quelques expérimentations à condition d'entourer ses expériences d'un suivi et d'un contrôle qui permettra précisément une évaluation *in vivo* des bienfaits de ces technologies et des balises, le cas échéant à mettre à leurs développements.

42. D'une approche basée sur les risques et fondée sur l'analyse de la finalité – L'approche par les risques conduit à créer des obligations nouvelles lorsque certains critères proposés par la réglementation indiquent que des risques supérieurs sont présents. Cette approche, dictée par le principe de proportionnalité était déjà présente, mais de manière très limitée, dans les dispositions du RGPD : l'article 35 réserve l'obligation d'analyse d'impact aux seuls traitements présentant un « risque élevé » pour les droits et libertés des personnes physiques. La notion de « risque élevé » reste imprécise. Le règlement sur les dispositifs médicaux distingue de même en différentes classes les produits et services selon la finalité de leur utilisation et les risques liés à la santé et à la sécurité et soumet à des procédures d'évaluation de la conformité aux exigences de la régulation les classes de produits à « haut risque ». La même idée parcourt *l'AI ACT* qui distingue différentes catégories de systèmes d'IA. *L'AI Act* ou plutôt les travaux du *High Level Group of experts on AI* sur l'éthique de l'IA[212], auxquels se réfère constamment cette proposition, élargit les risques à prendre en considération lors de l'évaluation des applications de l'IA. Ainsi, à côté des risques encourus par nos libertés individuelles, s'ajoute la nécessité de prendre en considération les risques dits collectifs propres à un groupe déterminé ou non de personnes, les risques d'atteinte à la justice sociale et, au-delà, les risques sociétaux, comme ceux encourus par l'environnement, la démocratie, le respect de l'état de droit. On sait que les premiers travaux sur la responsabilité des systèmes d'IA[213] retiennent la même idée de différencier les responsabilités des 'producteurs' ou utilisateurs professionnels de système d'IA, selon la gravité des dommages que l'utilisation des systèmes peut causer.

L'approche par les risques induit une autre conséquence : elle justifie pleinement le passage d'une rédaction légale classique – fondée sur la définition de contenus comportementaux à respecter et, en cas de non-respect, sur la répression ou la sanction *a posteriori* des infractions à la réglementation – à une approche *a priori* fondée sur

technologique (2) du développement des capacités d'institutions phares comme les organismes de prospective et de surveillance et les organes consultatifs, et (3) des processus en matière de débats sociétaux, d'innovation inclusive et de collaboration. » ou dans le domaine des données génétiques, le *« Genetic Act »* (GINA) américain (*The Genetic Information Non-discrimination Act of 2008* (Pub.L. 110–233 (text), 122 Stat. 881, enacted May 21, 2008, GINA), présenté par Wikipedia comme suit : "*GINA is an Act of Congress in the United States designed to prohibit some types of genetic discrimination. The act bars the use of genetic information in health insurance and employment : it prohibits group health plans and health insurers from denying coverage to a healthy individual or charging that person higher premiums based solely on a genetic predisposition to developing a disease in the future, and it bars employers from using individuals' genetic information when making hiring, firing, job placement, or decisions on promotion »*

[211] Cette approche est par ailleurs préconisée mais encadrée par la proposition *AI Act*.

[212] HLGE (High Level Group of experts) on AI, *Lignes directrices en matiere d'ethique pour une IA digne de confiance*, 8 avril 2019, no 67, texte disponible sur le site : Ethics guidelines for trustworthy AI – Publications Office of the EU (europa.eu).

[213] Rapport du groupe d'experts sur la responsabilité et les nouvelles technologies, section « nouvelles technologies », du 21 novembre 2019 et sur la responsabilité en matière d'intelligence artificielle et d'autres technologies numériques émergentes : *Liability for Artificial Intelligence and other emerging digital technologies*. La Commission européenne semble vouloir reprendre les idées de cette proposition de règlement à travers une modification profonde de la Directive de 1985 sur la responsabilité du fait des produits défectueux.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

l'obligation d'évaluation des risques, soit la mise sur pied d'une procédure en la matière et du contrôle du respect de cette procédure. L'approche préventive fondée sur les risques semble être une caractéristique des textes réglementaires européens récents. L'exemple déjà cité du « *Privacy Impact Assessment* », introduit par le RGPD, déplace ainsi le champ d'intervention de la réglementation vers une démarche préventive d'écartement des risques par la nécessité de mise sur pied d'une procédure d'évaluation dès la conception du traitement. La même idée traverse les autres règlements cités au paragraphe précédent. En particulier, la proposition *d'AI Act* développe à loisir cette procédure, définissant ses étapes, son contenu, insistant sur la participation de tous les acteurs intéressés, etc. On louera cette manière de faire, certes plus lourde administrativement et qui ne peut être justifiée que dans les cas de risques importants.

43. Un cadre réglementaire européen, incertain et complexe – Notre analyse du cadre réglementaire des systèmes d'IA utilisés dans le domaine médical s'est limité aux seuls RGPD, règlement sur les dispositifs médicaux et la proposition *d'AI Act*. Sans doute, bien d'autres points eussent pu être abordées, des législations sur les droits des patients, sur la bioéthique, sur l'agrément des médicaments et, au-delà, sur la cybersécurité, la responsabilité, les droits de propriété intellectuelle, voire sur la concurrence auraient pu être abordés. Notons tout d'abord l'importance prise par l'intervention de l'Union européenne et le peu de marge de manœuvre que les règlements que l'Union adopte laisse désormais aux solutions nationales, et ce, par la multiplication des règlements, là où l'Europe se contentait jusqu'il y a peu de directives. On ne cachera pas que cette intervention, si elle se réclame de la volonté de protéger des valeurs européennes, poursuit également un objectif économique, celui de créer un marché européen fort, tant grâce à une politique de certification et de labellisation que d'application extraterritoriale des prescrits et exigences réglementaires européens aux opérateurs étrangers. Le patient européen ne s'en plaindra pas. Nombre de textes créent ainsi des agences ou des autorités européennes en charge d'assurer la cohérence des actions des autorités nationales et de veiller à une interprétation et application uniformes des textes. Ceci dit, la prolifération d'autorités administratives créées par tous ces textes récents soulève des difficultés lorsqu'il s'agit d'analyser de manière transversale l'impact d'une technologie ou de se prononcer à l'occasion d'un litige qui met en cause les diverses thématiques envisagées séparément dans le cadre réglementaire et par des organes dont la culture et les prérogatives sont différentes. Cette situation fait craindre le nombre de prescrits et la lourdeur des contrôles administratifs que les opérateurs des systèmes d'IA auront à respecter. Par ailleurs, on peut craindre des tensions entre ces diverses autorités, ainsi, les autorités de protection des données réclament que soit élargie leur compétence à l'ensemble des exigences réclamées par *l'AI Act* aux systèmes d'IA.

44. Une intelligence artificielle ou des artifices de l'intelligence – Sans doute, les promesses de l'intelligence artificielle, en particulier dans le domaine de la santé, invitent à lui confier de plus en plus le soin de nos corps. Mais encore faut-il se rappeler qu'il ne s'agit là, au sens propre, que d'artifices de notre intelligence humaine et qu'à ce titre nous devons nous nous méfier des raccourcis que souvent notre cerveau emprunte et qui conduisent à tant de biais et d'erreur. Que ces technologies soient dignes de

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598

notre confiance (*Trustworthy AI*), exige notre prudence et notre maîtrise. C'est cette prudence et cette maîtrise continues qui constituent les mots-clés du droit européen naissant de l'intelligence artificielle. Au-delà des risques engendrés pour la santé de chacun de nous, au-delà des risques engendrés par l'utilisation des données de santé vis-à-vis de nos libertés individuelles, apparaissent des questions plus fondamentales, celles de notre identité, celles de notre dignité, celles du rôle irremplaçable de la relation humaine au sein du dialogue patient/soignant, celles enfin des risques d'une société à deux vitesses dans le droit à la santé, celles enfin des limites de la notion de santé. A toutes ces questions, il est nécessaire qu'un débat collectif multidisciplinaire et multipartite réponde. C'est le modeste rôle de l'universitaire de rappeler à l'Etat son devoir essentiel d'organiser ce débat, d'écouter et de décider ensuite sans *a priori,* sans craintes exagérées mais également sans aveuglement sur ce qui n'est jamais qu'un artifice de notre intelligence.

Published in : PIATTI, M-Ch. ; VIOLET, F. (dir.), *Pour des Intelligences artificielles au service du corps vulnérable*, Editions des archives contemporaines, ISBN : 9782813004598, doi : 10.17184/eac.9782813004598