



NOTE DE POSITION

INTELLIGENCE ARTIFICIELLE ET SOINS DE SANTÉ : LA QUESTION DES DROITS HUMAINS

Approuvée en séance plénière
du 09/02/2026

RESUME

La montée en puissance de l'intelligence artificielle (IA) et son utilisation dans les soins de santé ont amené le CSNPH à se poser la question des **enjeux de cette évolution technologique du point de vue des personnes en situation de handicap**. Le CSNPH a pris le temps nécessaire à l'examen de la documentation disponible sur le sujet. Il a par ailleurs rencontré des spécialistes de l'IA issus de la médecine, des hôpitaux, du droit, de la protection des droits humains, ainsi que des représentants des personnes en situation de handicap elles-mêmes.

Le cadre normatif encadrant l'IA est foisonnant mais inégal : d'un côté, des recommandations internationales (Conseil de l'Europe, Parlement Européen, Nations-Unies) qui fixent des **balises fortes** — non-discrimination, transparence, surveillance humaine — **sans valeur contraignante** ; de l'autre, des **instruments obligatoires** (AI-Act, RGPD, NIS2, loi anti-discrimination et loi relative aux droits du patient) **dont la portée reste partielle**. En particulier, l'AI-Act organise surtout la conformité des « produits » d'IA ; il ne crée pas de recours individuel pour atteinte aux droits fondamentaux, renvoyant de facto au RGPD ou à la loi anti-discrimination. Or, aussi bien l'AI-Act que le RGPD sont menacés de **révisions**, dans le cadre du projet Digital Omnibus de la Commission Européenne, **qui pourraient affaiblir la protection effective des citoyens**. Quant à l'Espace européen des données de santé, il généralise la circulation et la réutilisation des données de santé, tout en basculant d'un consentement explicite vers un consentement présumé — un renversement **qui fragilise le pouvoir d'agir des patients**.

Sur le plan éthique et juridique, la relation de soin doit rester un lien d'humain à humain. Jusqu'à présent, la décision médicale, avec ou sans recours à l'IA, demeure sous la responsabilité du médecin. Mais **l'IA pourrait à l'avenir déplacer le « standard of care » et devenir la norme de soins**. Qu'en est-il alors de la **responsabilité** en cas d'erreur et de la **relation de confiance entre le patient et son prestataire de soin** ? D'où l'appel du CSNPH à des mécanismes de validation centralisés des IA médicales (à la manière des médicaments), à des tests de biais obligatoires avant toute mise en service, et à des chartes déontologiques qui garantissent information loyale, supervision humaine et véritable consentement éclairé.

L'usage de l'intelligence artificielle en soins de santé menace également la littératie en soins de santé, déjà faible parmi les citoyens en Belgique. Accéder à l'information, comprendre, juger de la fiabilité et de la pertinence sont des compétences nécessaires pour pouvoir exercer ses droits en tant que patient et opérer ses propres choix en matière de santé. Or **l'introduction de l'intelligence artificielle dans l'exercice de la médecine rend plus difficile encore la compréhension des choix médicaux proposés par les prestataires de soins**. A cela s'ajoute le fait que les dispositifs d'IA ne sont pas toujours explicables, indépendamment des capacités du patient à comprendre et de la volonté du praticien à expliquer. **A travers la littératie en soins de santé, c'est le libre exercice des droits du patient qui est mis en danger**.

Sur le plan technique ensuite, trois nœuds critiques ressortent. Tout d'abord, **la qualité méthodologique du développement des systèmes d'IA** : il est crucial que les exigences de qualité soient **alignées sur les postulats de rigueur scientifique de la recherche médicale** : diversité des échantillons, transparence sur les méthodes et les métriques, tests externes et audits indépendants, documentation utilisable par les cliniciens et explicable aux patients. Deuxièmement, les **biais** : si les biais a posteriori, permettant de personnaliser le soin en fonction par exemple du handicap, de l'âge, de telle ou telle pathologie, peuvent être bénéfiques au patient à condition d'y inclure aussi le contexte spécifique de la personne, il n'en va pas de même des biais a priori, résultant des choix de développement. **Ces derniers peuvent avoir pour conséquence d'exclure des groupes de personnes**, ayant certaines pathologies par exemple, avec des conséquences sur l'adéquation des prestations de santé qui seront octroyées à ces bénéficiaires. L'outil médical basé sur une IA doit rester critiquable en permanence par le soignant : savoir à qui il s'applique, quand s'en écarter et comment justifier une décision humaine différente. Troisièmement, la **formation** : **sans montée en compétences continue des prestataires de soins, on glisse vers une médecine à deux vitesses**, contraire au droit à des soins de qualité pour tous.

Au-delà des cliniciens et des développeurs, la question de la **gestion des données** concentre d'autres

enjeux : **localisation** (serveurs vs cloud), **anonymisation** des données parfois impossible (par exemple pour les maladies rares), **cybersécurité**, **traçabilité** des usages, et **droits** effectifs des personnes. L'Espace Européen des données de santé, en instaurant le partage sans limite des données médicales à l'échelle européenne, balaie le droit à consentir des patients. Enfin, aucun devoir n'est assigné en contrepartie aux acteurs qui accèdent aux données.

De même, **le financement des projets d'IA en Belgique interpelle** : projets publics fragmentés, dépendances à des partenariats privés (p. ex. pharmaceutiques) qui peuvent interrompre les financements, et charges nouvelles des hôpitaux (registres d'IA, audits, créations de nouveaux rôles liés à la cybersécurité) non compensées par des budgets additionnels. **Au final, c'est le citoyen qui finance l'innovation technologique** : par la valeur monétaire de ses données de santé, par l'argent public à travers ses impôts, puis par ses dépenses en tant que patient.

Face à l'irruption de l'IA en soins de santé, le CSNPH plaide pour un réalisme exigeant. **Oui, l'IA peut améliorer la qualité des soins** : aide au diagnostic (imagerie, signaux faibles), personnalisation thérapeutique (profils génétiques, allergies), dépistage et prévention à l'échelle populationnelle, délestage de tâches administratives au bénéfice du temps clinique. **Mais ces gains supposent des garde-fous solides, car les risques sont concrets** : erreurs et biais, discriminations dans l'accès ou l'orientation des soins, opacité des modèles, atteintes à la vie privée et aux droits du patient, sécurité des systèmes et gouvernance des données encore insuffisantes.

De manière générale, le CSNPH constate une **érosion des protections des droits**. Droits individuels tout d'abord : l'IA et les algorithmes entraînent une **asymétrie de pouvoir et de connaissances**, au détriment de l'individu, ainsi qu'une **asymétrie dans l'exercice des droits et des devoirs**. L'intelligence artificielle engendre également des risques pour des groupes d'individus exposés plus que d'autres aux discriminations algorithmiques. Or l'arsenal juridique ne se développe pas aussi vite que la technologie, la « discrimination collective » n'est pas traduite dans la réglementation.

A l'issue de son analyse, le CSNPH formule une série de recommandations : renforcer — plutôt qu'affaiblir — les **droits** (recours individuels, droits du patient, RGPD), rendre opposables certaines exigences aux IA « à risque modéré », compléter l'AI-Act par des **contraintes sectorielles santé** (méthodologie, validation, gouvernance des données), financer la **formation IA continue des soignants**, développer des **modèles ouverts** adaptés aux pathologies fréquentes et rares, **soutenir la cybermaturité des hôpitaux**, instaurer la **traçabilité** individuelle des données et informer automatiquement tout citoyen lorsqu'une décision le concernant a intégré un algorithme. L'objectif n'est ni de freiner l'innovation ni de l'idéaliser : il s'agit d'organiser une innovation sûre, équitable et explicable, **où la technologie soutient la qualité des soins sans rogner la liberté et les droits des patients**.

SOMMAIRE

Contexte	
Méthodologie.	
L'intelligence artificielle et le cadre général, national, européen et international : lois, directives, conventions.....	
1°) Les droits humains comme balises de l'IA... des recommandations malheureusement non contraignantes.....	
2°) Un cadre contraignant... insuffisant ou remis en question.....	
L'intelligence artificielle en soins de santé : impacts et enjeux.....	
Concrètement, l'intelligence artificielle dans les trajets de soins.....	
Conclusions et recommandations.....	
Glossaire.....	

0/ Préambule

Les évolutions et applications dans le domaine de l'intelligence artificielle sont très rapides et nombreuses. Dans ce contexte, la présente note ne prétend pas être exhaustive et est appelée à être mise à jour ultérieurement.

1/ Contexte

En 2017, le CSNPH avait déjà consacré une [note de position](#) consacrée aux soins de santé et, plus particulièrement, aux nombreux défis auxquels les personnes en situation de handicap ou de maladie chronique sont confrontées dans ce secteur. A cette occasion, le CSNPH pointait un certain nombre d'attentes et formulait plusieurs recommandations, parmi lesquelles la préservation de la **dignité**, **l'accessibilité** financière et **technologique**, la **continuité des soins**, l'autonomie des **choix** de vie et la **responsabilité des professionnels** dans le cas d'une délégation des actes de soin.

Nous sommes en 2026 et le contexte a changé. La montée en puissance de l'IA et son utilisation dans les soins de santé ont amené le CSNPH à se poser la question des enjeux de cette évolution technologique du point de vue des personnes en situation de handicap. Selon la définition de l'AI-Act, un « système d'IA » est *« un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites et implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels »* (article 3, 1). L'IA se développe à une allure très rapide et semble brûler les étapes, notamment celle de la réflexion, pourtant nécessaire. Le CSNPH a voulu s'arrêter sur le phénomène pour mieux le comprendre et réfléchir aux besoins des personnes en situation de handicap ou de maladie chronique dans un contexte de « médecine augmentée ».

2/ Méthodologie

LE CSNPH a pris le temps nécessaire à l'examen de la documentation (livres, articles, webinaires, formations) sur le sujet de l'intelligence artificielle en soins de santé. Il a par ailleurs rencontré et auditionné :

- un expert académique actif dans la formation en intelligence artificielle des professionnels de la santé ;
- des médecins directement confrontés à l'IA dans leurs pratiques quotidiennes ;
- un *Data Protection Officer* (DPO) et *Chief Information Security Officer* (CISO) d'un important complexe hospitalier belge ;
- des juristes spécialisés en intelligence artificielle, en protection des données et en droits des patients ;
- des personnes en situation de handicap elles-mêmes ;
- des associations belges et européenne représentatives de personnes en situation de handicap ;
- des représentants d'institutions actives dans le domaine de la protection et la défense des droits humains.

La présente note de position est le résultat de ce travail de fond, participatif et largement représentatif des réalités de vie de toutes les régions du pays.

3/ L'Intelligence artificielle et le cadre général, national, européen et international : lois, directives et conventions

Bien que l'intelligence artificielle soit une innovation technologique relativement récente, nombreuses sont les conventions, lois, directives, qui balisent sa conception, son déploiement et son utilisation. Certaines sont contraignantes et d'autres pas. Certaines concernent les aspects techniques et les produits à base d'IA ; d'autres cherchent à définir un périmètre de jeu, respectueux des droits humains, dans lequel l'IA devrait se développer.

A. Les droits humains comme balises... des recommandations malheureusement non contraignantes

L'intelligence artificielle et les droits humains : les recommandations du Conseil de l'Europe

Le Conseil de l'Europe, en sa qualité de défenseur des droits humains¹, a publié plusieurs textes concernant, de près ou de loin, l'intelligence artificielle, dont :

- la Recommandation du Conseil des Ministres aux Etats Membres sur les impacts des systèmes algorithmiques sur les droits humains du 8 avril 2020 ([CM/Rec 2020/1](#))
- la Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'Etat de droit du 5 septembre 2024 ([STCE 225](#)).

1°) Recommandation du Conseil des Ministres aux Etats Membres sur les impacts des systèmes algorithmiques sur les droits humains du 8 avril 2020 (CM/Rec 2020/1)

Face à la place grandissante des outils numériques dans la vie quotidienne, et notamment dans les soins de santé, le Conseil des Ministres du Conseil de l'Europe a adressé plusieurs recommandations aux Etats Parties :

- En matière législative : **créer et adapter les cadres législatifs** concernant les systèmes algorithmiques afin de garantir leur **conformité aux droits humains**, en concertation avec les parties prenantes, dont la **société civile**. Il s'agit notamment d'accorder « *une attention particulière aux besoins et voix des **groupes vulnérables**, pour veiller à ce que l'impact sur les droits de l'homme engendré par la conception, le développement et le déploiement en cours de systèmes algorithmiques fassent l'objet d'un suivi, d'un débat et d'une solution* » (5^e recommandation).
- En matière de contrôle : créer ou promouvoir des **institutions nationales de surveillance, de contrôle, d'évaluation des risques** en leur attribuant les ressources nécessaires pour contrôler, superviser et coordonner le respect de ce cadre législatif.
- En matière de communication : veiller à la **diffusion** la plus large possible de la recommandation aux parties prenantes.
- En matière d'éducation : encourager et promouvoir des **programmes d'éducation aux médias et au numérique**, de manière à réduire au minimum l'exposition aux dangers et de façon à permettre à chacun de comprendre les systèmes de décision automatisée et de prendre des décisions éclairées.

Ces recommandations se déclinent dans des obligations concrètes pour la mise en place de ces principes généraux. Parmi ces obligations, citons entre autres :

- Création de cadres institutionnels et réglementaires établissant **des critères et des garanties** pour assurer la compatibilité des systèmes algorithmiques avec les droits humains.
- **Elaboration et évaluation des lois et des politiques** impliquant de **consulter** régulièrement toutes les parties prenantes concernées.
- Doter les **autorités de régulation et de contrôle** de ressources et d'expertise suffisantes.
- Evaluation, tout au long de leur cycle de vie, des algorithmes par la **mise en place de tests et d'audits réguliers**, en ce comprises des **études d'impact des systèmes algorithmiques sur les droits**

¹ Le Conseil de l'Europe est une organisation de défense des droits humains, née en 1946, qui repose sur la Convention européenne des droits de l'homme (CEDH). Cette organisation compte 46 états membres et représente 700 millions de citoyens.

humains, réalisés par des experts indépendants, en vue de contrôler la pertinence, le respect de la vie privée, la protection des données, les effets discriminatoires et le respect des droits humains. « Toute limitation importante des droits humains qui serait décelée lors de la mise à l'essai de ces systèmes devrait donner lieu à une **rectification immédiate** et, à défaut, à la **suspension du système** en attendant que ces corrections puissent avoir lieu ». (Obligation 3.3) Une **attention particulière doit être accordée aux résultats biaisés ou discriminatoires**. Par ailleurs, les évaluations et essais doivent porter sur des échantillons de population suffisamment représentatifs et diversifiés afin de réduire les risques de discrimination.

- Devoir pour les acteurs du secteur privé d'**impliquer des associations de consommateurs, des défenseurs des droits humains et d'autres organisations** représentant les intérêts des individus et groupes concernés dans les processus de conception, développement, déploiement et évaluation des systèmes algorithmiques.
- Création de systèmes de **certification** pour garantir la provenance et la qualité des jeux de données et des modèles.
- Imposer des normes élevées de transparence et d'explicabilité par le biais de **labels éthiques** pour les systèmes algorithmiques.
- Renforcer la **responsabilité des acteurs du secteur privé en matière de droits de l'homme et de libertés fondamentales**. « Il appartient [au secteur privé] de veiller à ce que la conception, le développement ou le déploiement en cours de leurs systèmes algorithmiques n'aient pas de conséquences discriminatoires directes ou indirectes sur les individus et les groupes concernés, notamment sur ceux qui ont des besoins particuliers ou un **handicap**, ou qui pourraient rencontrer des **inégalités structurelles** dans leur accès aux droits de l'homme » (Principes d'application générale 1.4)
- Financer des recherches technologiques indépendantes pour élaborer des **mécanismes permettant d'évaluer les systèmes algorithmiques**.
- Assurer la **formation en matière de non-discrimination et de respect des droits de l'homme** du personnel chargé de développer, mettre en œuvre, évaluer ou contrôler les systèmes algorithmiques.
- Garantir la **traçabilité** des décisions algorithmiques.
- **Sensibiliser le public** à l'utilisation potentielle des systèmes algorithmiques pour manipuler, exploiter, tromper ou répartir les ressources en vue de permettre aux individus et aux groupes de **mieux connaître leurs droits**.
- Garantir le droit à l'**autodétermination informationnelle** en veillant à ce que les individus soient **informés à l'avance** du traitement de leurs données et en leur offrant la possibilité de **contrôler** leurs données, en ce compris de les **invisibiliser**.
- Garantir le droit à **consentir** et à **retirer son consentement** à l'utilisation de ses données, tout en maintenant l'accès aux services.
- Mettre en place des **points de contact et de permanence téléphonique faciles d'accès** pour favoriser la contestation et former, sur les normes en matière de droits de l'homme, le personnel chargé de recueillir les plaintes.
- Prévoir des possibilités effectives d'introduction de **plaintes** ou de **recours** via des procédures judiciaires et non judiciaires **équitables, faciles d'accès, abordables et indépendantes**.

Ces recommandations n'ont pas de caractère contraignant.

2°) Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'Etat de droit du 5 septembre 2024 (STCE 225)

Quatre ans après les recommandations qui précèdent, le Conseil de l'Europe propose à la signature et à la ratification une convention-cadre. Celle-ci fait part des préoccupations du Conseil de l'Europe face aux **risques de discrimination et d'aggravation des inégalités** auxquels les systèmes d'intelligence artificielle exposent « **les personnes en situation de vulnérabilité** ». Elle énumère des principes généraux pour une

utilisation de l'intelligence artificielle conforme aux grands traités internationaux, dont la Déclaration universelle des Droits de l'Homme, la Charte sociale européenne révisée et la **Convention des Nations Unies relatives aux droits des Personnes Handicapées**. La convention-cadre s'applique aussi bien aux pouvoirs publics qu'aux acteurs privés.

Les principes généraux appliqués aux activités menées dans le cadre de vie des systèmes d'intelligence artificielle sont les suivants : **la dignité humaine et l'autonomie personnelle, la transparence et le contrôle, la responsabilité pour les impacts négatifs sur les droits humains, l'égalité et la non-discrimination, le respect de la vie privée et la protection des données à caractère personnel, la fiabilité des systèmes et des résultats, une innovation sûre, des droits de recours contre les violations des droits humains incluant un droit à une information pertinente et suffisante pour introduire une plainte.**

La convention-cadre fait explicitement référence aux **droits des personnes en situation de handicap** mais en restreint malheureusement la portée en prévoyant pour les Etats Parties la possibilité de se conformer à leur droit national (chapitre IV, article 18).

Enfin, le texte de la convention instaure une obligation de rapport périodique des Etats Parties sur leurs avancées en matière d'intelligence artificielle et de respect des droits humains.

15 pays ont signé la Convention, dont 10 membres du Conseil de l'Europe, mais aucun d'eux ne l'a ratifiée. Or l'article 30 prévoit une entrée en vigueur du traité trois mois après que 5 pays, dont 3 membres au moins du Conseil de l'Europe, l'auront ratifié. La Convention n'est donc pas entrée en vigueur. **La Belgique ne l'a ni signée, ni ratifiée.**

L'Union Européenne affirme un nouveau concept : les « droits numériques »

La [*Déclaration européenne sur les droits et principes numériques pour la décennie numérique*](#)² répond aux préoccupations du Parlement Européen qui souhaitait que la **Deuxième Stratégie numérique de l'Union Européenne 2021-2030** s'inscrive dans le **respect des valeurs européennes et des droits fondamentaux**. Conformément à cette attente, la Déclaration s'ouvre dès l'article premier sur le rappel de **l'Union des Valeurs et de la Charte des Droits fondamentaux**. Les différents chapitres se déclinent selon les valeurs de solidarité et **inclusion** (chapitre II), **liberté de choix** (chapitre III), **participation** à l'espace public (chapitre IV), **sûreté**, **sécurité et autonomisation** (chapitre VI), durabilité (chapitre VII) et insiste sur la nécessité de « mettre les citoyens au cœur de la transformation numérique » (chapitre I).

En ce qui concerne l'intelligence artificielle, la Déclaration stipule à l'article 9 que « *Toute personne devrait être en mesure de bénéficier des avantages qu'offrent les systèmes algorithmiques et d'intelligence artificielle, y compris en faisant des **choix libres et éclairés** dans l'environnement numérique, **tout en étant protégée contre les risques et les atteintes à sa santé, à sa sécurité et à ses droits fondamentaux*** ». A cet égard, les Parlement, Conseil et Commission européens s'engagent notamment à :

- *veiller à ce que les systèmes algorithmiques reposent sur des ensembles de **données appropriées**, afin d'**éviter toute discrimination***
- *permettre une **surveillance humaine** de tous les résultats qui affectent la sécurité et les droits fondamentaux des citoyens*
- *veiller à ce que les technologies telles que l'intelligence artificielle ne soient **pas utilisées pour préjuger des choix des personnes**, par exemple en matière de **santé**, d'éducation, d'emploi et de **vie privée**.*

La Déclaration insiste en outre sur certains grands principes, en particulier :

- que la transformation numérique ne doit laisser personne de côté et cite, parmi d'autres, « **les personnes handicapées** ou les personnes marginalisées, **vulnérables** ou défavorisées et **les personnes qui agissent en leur nom** »

² La Déclaration européenne sur les droits et principes numériques pour la décennie numérique est publiée au *Journal Officiel de l'Union Européenne* le 23 janvier 2023. Elle est le fruit d'une concertation entre le Parlement Européen, le Conseil Européen et la Commission Européenne. Elle s'inscrit dans le cadre de la Deuxième Stratégie numérique de l'Union Européenne 2021-2030, qui fixe quatre objectifs principaux : des infrastructures numériques sûres, la transformation numérique des entreprises, la numérisation des services publics et la montée en compétence numérique des professionnels de l'Union Européenne.

- le **droit à la vie privée** et au **contrôle de ses données personnelles**
- la nécessité d'avoir accès à des **informations exactes et faciles à comprendre** afin de garantir la possibilité à chacun d'exercer sa liberté de choix.

Cette Déclaration n'est pas plus contraignante que les recommandations ou la Convention du Conseil de l'Europe.

Les recommandations des Nations-Unies à la Belgique

La Belgique est signataire et Etat Partie de la **Convention relative aux droits des personnes handicapées** (UNCRPD) depuis 2009. Le Comité UNCRPD³, dans ses [observations finales 2024](#) concernant la Belgique, recommande d'incorporer la **loi de l'Union Européenne sur l'intelligence artificielle** dans le droit national et de mettre en place un **organisme de contrôle spécialisé dans les droits de la Convention, la protection des données et la vie privée** afin de superviser sa mise en œuvre.

B. Un cadre contraignant... insuffisant ou remis en question

L'AI-Act

Le Règlement établissant des règles concernant l'intelligence artificielle, appelé aussi [AI-Act](#), est une réglementation européenne : elle est contraignante et doit être transposée en droit national par les différents pays de l'Union Européenne. Elle est entrée en vigueur le 01/08/2024. Un calendrier par étapes a été fixé pour sa mise en application, qui pourrait toutefois être reporté si les propositions du Digital Omnibus⁴ de la Commission Européenne sont adoptées. Les dates ci-dessous sont celles du calendrier actuellement en vigueur :

- Février 2025 : dispositions générales et pratiques interdites
- Août 2025 : objectifs généraux
- Août 2026 : dispositions concernant les systèmes d'IA à haut risque (éventuellement reportées à 2027 ou 2028)
- Août 2027 : application totale (à adapter en fonction d'un éventuel nouveau calendrier pour les systèmes d'IA à haut risque).

Le règlement s'applique aux **fournisseurs et déployeurs** de systèmes d'IA, qu'ils soient établis ou non dans l'Union européenne, aux **importateurs et distributeurs**, ainsi qu'aux **fabricants** qui embarquent un système d'IA dans leurs propres produits.

L'AI-Act propose une réglementation des systèmes IA basée sur une approche des risques. Quatre niveaux de risque sont déterminés : minime, limité, haut, inacceptable. Les risques inacceptables sont interdits. Sont considérés à haut risque les systèmes d'IA qui, de manière générale, « *peuvent perpétuer des schémas historiques de **discrimination**, par exemple à l'encontre des femmes, de certains groupes d'âge, **des personnes handicapées**, ou de certaines personnes en raison de leur origine raciale ou ethnique ou de leur orientation sexuelle* ». En matière de soins de santé, il s'agit des :

- systèmes d'IA « *destinés à être utilisés pour évaluer **l'éligibilité aux services de soins de santé** ainsi que pour octroyer, réduire, révoquer ou récupérer ces services* » (Annexe III, 5, a)
- systèmes d'IA « *destinés à évaluer et **hiérarchiser les appels d'urgence** [...] ou à être utilisés pour [...] **établir des priorités dans l'envoi des services d'intervention d'urgence, y compris [...] l'assistance médicale**, ainsi que pour les systèmes de **tri des patients** admis dans les services de santé* »

³ Le Comité des droits des personnes handicapées ou Comité UNCRPD est chargé de veiller au respect de la Convention. A intervalles réguliers, les Etats Parties soumettent à ce Comité un rapport mettant en évidence, pour leur pays, l'état d'avancement du respect des droits des personnes en situation de handicap. La société civile remet, de son côté, un rapport parallèle, dit alternatif. A la suite de ce dialogue avec le pays évalué et sa société civile, le Comité UNCRPD publie ses « observations finales ».

⁴ Le Digital Omnibus est un paquet de mesures proposées par la Commission Européenne visant à simplifier et harmoniser la législation numérique de l'Union Européenne. Sont notamment concernés : l'AI-Act et le Règlement Général de Protection des Données (RGPD).

d'urgence » (Annexe III, 5, d)

- systèmes d'IA « destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'**assurance-santé** » (considérant 56)

car « s'ils ne sont pas dument conçus, développés et utilisés, [ces systèmes] peuvent porter atteinte [aux] droits fondamentaux et entraîner de **graves conséquences pour [la] vie et [la] santé, y compris [...] la discrimination** » (considérant 56). Ces systèmes d'IA à haut risque sont soumis à un certain nombre d'obligations spécifiques qui pourraient toutefois être revues dans le cadre du Digital Omnibus de la Commission Européenne :

- mettre en place un système de **gestion des risques**, régulièrement révisé et mis à jour tout au long du cycle de vie de l'IA
- utiliser des **données de haute qualité**, complètes et exemptes d'erreur, pour minimiser les biais et garantir des résultats équitables et transparents
- être conçus pour être **précis, robustes et sûrs**, résistants aux erreurs et aux défaillances
- enregistrer les événements pertinents dans l'objectif d'**identifier les risques** et retracer les modifications substantielles
- garantir une **surveillance humaine** afin de **prévenir ou minimiser les risques pour la santé** et la sécurité et **les droits fondamentaux** ; le personnel chargé de cette surveillance auprès du déployeur doit être en capacité d'exercer la tâche qui lui est confiée
- tenir à jour une **documentation technique détaillée** afin de prouver que le système respecte les prescrits légaux
- fournir des instructions d'utilisation claires et des informations sur **les capacités, les limites et les risques potentiels** du système
- réaliser une **analyse d'impact sur les droits fondamentaux**
- mettre en place un système de **gestion documentée de la qualité**
- faire l'objet d'une évaluation de **conformité par un tiers**
- être enregistrés dans la **banque de données centrale tenue par la Commission Européenne** et être **accessibles au public**.

Pour les IA générales, comme Chat GPT par exemple, considérées à risque limité, un code de bonne conduite a été publié le 10 juillet 2025, qui présente des obligations à respecter en matière de [sécurité](#), de [transparence](#) et de [droit d'auteur](#), mais ce code de bonne conduite n'est **pas contraignant**. C'est un « outil volontaire », selon les termes de la Commission, pour les fournisseurs qui cherchent à se conformer à la législation de l'AI-ACT et, en particulier, à l'article 55. Les fournisseurs qui adhéreront au code de bonne conduite seront récompensés par une réduction de leur charge administrative.

Entrent dans la catégorie d'IA générales les **chatbots** et les « **compagnons thérapeutiques** » qui, par conséquent, ne sont pas soumis aux règles de protection des systèmes d'IA à haut risque. Or les IA génératives sont programmées pour aller dans le sens de qui les interroge. En médecine, cela peut avoir des **conséquences graves**, si l'IA valide le souhait d'un patient d'arrêter ou de modifier son traitement par exemple⁵.

D'autres dispositions sont encore à épingler :

- l'article 3 (47) institue un « Bureau de l'IA », chargé de la supervision des systèmes d'IA et des IA générales, avec pouvoir d'enquête concernant les éventuelles infractions aux règles européennes
- les utilisateurs doivent être informés, lorsqu'ils interagissent avec une IA, qu'ils sont en train de le faire avec une IA.

L'AI-Act est surtout et avant tout une **réglementation qui porte sur les produits**. Certes, le règlement affirme, dès le considérant 1 et à l'article 1(2), son objectif de garantir une IA « digne de confiance », fondée sur les valeurs de l'Union Européenne, en assurant un haut niveau de protection des droits fondamentaux consacrés par la Charte des Droits fondamentaux (2000/C 364/01), parmi lesquels on

⁵ Cette remarque concerne l'IA générative et les compagnons thérapeutiques qui relèvent de réglementations lacunaires. En revanche, lorsque les chatbots sont conçus pour mener des discussions médicales ou un suivi de patient, ils sont réglementés au même titre qu'un autre dispositif médical. Il s'agit de deux produits différents, soumis à des réglementations différentes.

retrouve notamment la dignité humaine, la vie privée et la protection des données, la non-discrimination, les droits des personnes en situation de handicap et l'accès à la justice. Toutefois, si les droits fondamentaux sont rappelés dès les premières lignes du texte, **l'AI-Act prévoit bien peu pour les protéger** :

- **Aucune procédure** n'est prévue pour introduire une **plainte** en cas de violation de ces droits fondamentaux. Et **aucune réparation**, ni financière ni d'aucune sorte, n'est due.
- L'article 86 octroie à toute personne « *faisant l'objet d'une décision prise par un déployeur sur la base des sorties d'un système à haut risque [...] et qui produit des effets juridiques ou affecte significativement cette personne [...] d'une manière qu'elle considère comme ayant des conséquences négatives sur sa santé, sa sécurité ou ses droits fondamentaux* » le seul droit « *d'obtenir du déployeur des explications claires et pertinentes sur le rôle du système d'IA dans la procédure décisionnelle et sur les principaux éléments de la décision prise* » (article 86).
- « *les autorités ou organismes publics nationaux qui supervisent ou font respecter les obligations [...] visant à protéger les droits fondamentaux, y compris le droit à la non-discrimination, en ce qui concerne les systèmes d'IA à haut risque [...] sont habilités à demander toute documentation créée ou conservée [...] et à y avoir accès dans une langue et un format accessibles lorsque l'accès à cette documentation est nécessaire à l'accomplissement effectif de leur mandat dans les limites de leurs compétences* » (article 77). Dans cette perspective, chaque Etat membre devait identifier, pour le 2 novembre 2024, le ou les organismes désignés pour ce faire. Pour la Belgique, **pas moins de 27 organismes ont été nommés**, dont 14 fédéraux, 3 pour la Communauté Française, 2 pour la Communauté Germanophone, 2 pour la Région wallonne et 6 pour la Flandre⁶.
- Ces organismes nommés ne peuvent introduire de plainte que dans le cadre de la **loi anti-discrimination belge**, et pas dans le cadre de l'AI-Act.
- Ces organismes nommés n'ont qu'un **rôle consultatif** au regard de l'AI-Act.

En l'absence de recours individuel prévu par l'AI-Act en cas de violation des droits fondamentaux, les personnes qui s'estimeraient victimes de telles violations devraient tout d'abord demander des informations au fournisseur, avec l'aide éventuelle de l'un des 27 organismes désignés pour la protection des droits humains pour avoir accès à la documentation du système incriminé. Sur la base du dossier ainsi constitué, **elles ne pourraient introduire de plainte que dans le cadre d'autres réglementations en vigueur, comme le RGPD ou la loi anti-discrimination par exemple.**

Le RGPD

Le règlement européen 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, est entré en vigueur le 25 mai 2018. Il est **contraignant**. Il a pour objectif de **permettre aux individus de mieux contrôler leurs données à caractère personnel** et institue un système d'autorités de supervision indépendantes chargées de surveiller et de faire respecter l'application de cette réglementation. En Belgique, cette autorité, créée par la loi du 3 décembre 2017, s'appelle **Autorité de Protection des Données (APD)**. Par « donnée personnelle », on entend « *toute information se rapportant à une personne physique identifiée ou identifiable* ». Le « traitement des données », pour sa part, renvoie à « *toute opération effectuée sur ces données à caractère personnel, telle que la collecte, l'utilisation, la gestion ou la communication* » ([Données personnelles | Belgium.be](#)).

Le RGPD garantit, pour les personnes, les droits suivants ([Quels sont mes droits ? | Autorité de protection des données](#)) :

- Droit à être informé sur la **finalité** de la collecte des données personnelles, le **temps de conservation**, les **tiers** auxquels ces données sont transmises et la base juridique sur laquelle les données sont traitées
- Droit d'**accès** à ses données personnelles, en ce compris le droit à en recevoir une **copie**
- Droit de **rectification** des erreurs ou des données qui ont changé (comme une adresse de domicile par exemple)

⁶ Pour la liste des 27 organismes, voir [Intelligence artificielle | SPF Economie](#) et [Artificielle intelligente | FOD Economie](#).

- Droit de **transfert** des données d'une organisation vers une autre : la première organisation ne peut s'y opposer
- **Consentement éclairé**, étant entendu que le consentement est défini comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »
- Droit de **retirer son consentement** à tout moment sans avoir à se justifier
- Droit d'**effacement**, ou droit à l'oubli, lorsqu'une personne ne souhaite plus que ses données soient traitées et qu'il n'y a pas de motif légitime de les conserver, ou lorsque les données ont été obtenues sans consentement explicite ou de la part d'une personne mineure
- Droit de **s'opposer au traitement de ses données à caractère personnel**, hors raison impérieuse, **et aux décisions automatisées**. Dans ce dernier cas, une organisation ne peut prendre aucune décision concernant la santé ou la situation financière de la personne qui a manifesté son opposition, qui porterait uniquement sur la base des informations personnelles, en l'absence d'intervention humaine
- Droit à la **limitation** du traitement en cas d'inexactitude des données, en cas d'obtention illicite ou lorsque leur conservation n'est plus nécessaire
- Droit de **savoir quand ses données à caractère personnel ont été violées** : les entreprises et les organisations ont l'obligation d'informer l'APD et, en cas de violation grave, les personnes concernées

Parmi les obligations imposées aux entreprises, citons :

- **Analyse d'impact sur la protection des données** lorsque le traitement des données peut engendrer un risque élevé pour les droits et libertés des personnes physiques
- Tenue de **registres** pour les traitements réguliers ou susceptibles d'engendrer un risque pour les droits et libertés des personnes physiques

Finalement une disposition de loi qui définit et protège les droits des citoyens ? C'est sans compter le projet de refonte du RGPD, aujourd'hui objet de discussions. A la suite de la publication du « rapport Draghi », en septembre 2024, qui cite le RGPD comme un « frein à l'innovation et à la compétitivité », la Commission Européenne a décidé de revoir cette législation et de présenter une **proposition de réduction (« Disruption » – Innovation technologique ou vie privée : la Commission ouvre la boîte de Pandore - [Le Soir](#))**. Cette réduction pourrait avoir des conséquences sur l'AI-Act puisqu'un citoyen s'estimant victime d'un dispositif d'intelligence artificielle et lésé dans ses droits n'a la possibilité d'introduire une plainte ou un recours qu'à travers des législations connexes, dont précisément le RGPD. Les propositions actuellement contenues dans le Digital Omnibus de la Commission Européenne visent en effet à limiter les droits d'accès, de consentement et d'opposition, en plus des analyses d'impact.

La protection des données : les précisions de la Cour Européenne de Justice et de l'Autorité belge de Protection des données

Afin de pouvoir exercer les droits que lui confère le RGPD, chacun doit pouvoir comprendre, pour lui-même, lesquelles de ses données sont utilisées, avec quelles finalités. Dans un arrêt du 7 mai 2009 ([Aff. C-553/07](#), §66), la Cour Européenne de Justice estime que **6 mois comme délai de conservation des données de traçage n'est pas suffisant** et demande de l'augmenter.

A signaler également, la recommandation de l'Autorité belge de Protection des données, dans son [avis 203/2022](#) du 9 septembre 2022 : l'APD, en s'appuyant sur la Convention Européenne des Droits de l'Homme, rappelle que **tout traitement de données à caractère personnel doit être prévisible**. « *Afin d'éviter l'application arbitraire de [...] méthodes d'enquête et de recherche, il importe que les personnes concernées puissent évaluer dans quels cas le datamining [exploration ou fouille de données] peut être et sera utilisé* » (alinéa 9).

Pas de protection des données sans sécurité des données : la loi dite « NIS2 »

En complément essentiel du RGPD, l'objectif de la loi⁷ est d'établir un **niveau élevé de cybersécurité**, de **renforcer la gestion des risques et des incidents** et supervise les entités fournissant des services essentiels. La loi vise également à coordonner les politiques publiques de cybersécurité. Le **Centre pour la Cybersécurité Belgique** (CCB) est désigné comme autorité nationale de cybersécurité.

Sont considérées comme entités fournissant des services essentiels et secteurs hautement critiques : **la santé**, l'infrastructure numérique, la gestion des services TIC et les administrations publiques entre autres. Ces entités ont l'obligation de :

- **S'enregistrer** auprès du CCB
- Prendre des **mesures de cybersécurité** adéquates
- Notifier au CCB les **cyberincidents** significatifs
- Effectuer des **évaluations régulières de la conformité**, laquelle est vérifiée par un organisme de contrôle de la conformité.

En règle générale, tout autre entité, dont les services sont considérés non essentiels, tombe en dehors du périmètre de la loi. Ainsi, les applications grand public ou les dispositifs d'IA utilisés à domicile ne sont pas couverts par ces dispositions légales. Il existe quelques exceptions :

- Si l'IA domestique dépend d'une infrastructure critique, l'opérateur de l'infrastructure entre dans le champ de la loi ;
- Si un acteur d'IA fournit des services considérés comme critiques, par exemple un prestataire TIC ou un fournisseur de services numériques essentiels, il pourrait être soumis à la loi même si ses produits sont utilisés à domicile.

La loi anti-discrimination

La loi anti-discrimination du 10 mai 2007, tend à lutter contre certaines formes de discriminations. Elle s'applique entre autres à la **fourniture de biens et de services mis à disposition du public**. La loi interdit toute discrimination fondée sur l'âge, l'orientation sexuelle, **l'état de santé, le handicap, une caractéristique physique ou génétique** entre autres, qui constituent des « critères protégés » : toute discrimination sur la base d'un ou de plusieurs de ces critères peut donner lieu à une condamnation. Par ailleurs, la loi reconnaît plusieurs formes de discriminations :

- **Directe** quand une personne est traitée moins favorablement qu'une autre en raison de l'un ou de plusieurs des critères protégés
- **Indirecte** lorsqu'une disposition apparemment neutre est susceptible d'entraîner un désavantage pour les personnes caractérisées par l'un ou l'autre des critères protégés
- **L'injonction à discriminer** une personne, un groupe, une communauté sur la base d'un ou de plusieurs critères protégés
- **Harcèlement**, soit tout comportement lié à un ou plusieurs critères protégés portant atteinte à la dignité de la personne et créant un environnement intimidant, hostile, dégradant, humiliant ou offensant.

En cas de discrimination, la loi prévoit que la victime peut réclamer des **dommages et intérêts** ou introduire une **action en cessation**. Dans ce dernier cas, la victime peut prétendre à une indemnité forfaitaire. **La charge de la preuve repose sur la personne incriminée**. Toutefois, la victime doit apporter des éléments concrets appuyant le bien-fondé de sa plainte. La personne victime de discrimination peut signaler sa situation auprès d'un organisme habilité par la loi, tel qu'Unia, qui l'aidera à préparer son dossier.

Les Communautés et Régions, dans le cadre de leurs pouvoirs, peuvent également prendre des décrets ou ordonnances sur le sujet des discriminations.

En 2023, une nouvelle loi est venue compléter l'ancienne et reconnaît désormais **la discrimination par association**, lorsqu'une personne est traitée moins favorablement parce que l'on croit à tort qu'elle relève

⁷ Cette loi du 26 avril 2024 établit un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et est une transposition de la directive UE 2022/2555 du 14 décembre 2022. Elle est entrée en vigueur le 18 octobre 2024.

d'un ou de plusieurs critères protégés, ainsi que la **discrimination multiple** portant simultanément sur plusieurs critères protégés. Les montants des dommages et intérêts ont été relevés et s'élèvent à une fourchette comprise entre 2000 et 4000 euros.

La loi sur les droits du patient

En 2002, la Belgique s'est dotée d'une loi définissant les droits du patient à l'égard du professionnel qui lui apporte des soins. Elle a été modifiée par la loi du 6 février 2024, qui introduit de nouvelles dispositions en matière de santé et intègre des éléments de la loi de 2019 relative à la qualité des soins. La loi de 2024 se centre davantage sur l'intérêt du patient en insistant sur la **nécessaire prise en compte des objectifs de vie de ce dernier, de ses préférences et de ses valeurs**. Elle inclut également les possibilités de soutien pour le patient, que ce soit par une **personne de confiance** ou par un **représentant** au cas où le patient serait incapable d'exercer ses droits par lui-même. La philosophie de la loi vise à instaurer un **modèle de collaboration, de dialogue et de respect mutuel entre patient et soignant**.

Les droits résultants du patient sont les suivants :

- Droit à bénéficier d'une prestation de **soins de qualité**, à savoir des **meilleurs soins possibles en fonction des connaissances médicales et des technologies disponibles**. Ces soins respectent la dignité humaine et l'autonomie du patient, à travers notamment ses objectifs de vie, ses choix et ses valeurs.
- Droit à **choisir librement son prestataire** de soins, qui lui précise, sur demande, ses compétences et son expérience. Le prestataire de soins peut interrompre la relation de soins pour des raisons personnelles ou professionnelles, mais doit prendre les dispositions nécessaires pour garantir la continuité des soins.
- Droit à **être informé** sur son état de santé, à savoir le diagnostic et l'évolution probable. **L'information tient compte des capacités de compréhension du patient**.
- Droit de **consentir librement** à la prestation de soins, avec information préalable. Ceci implique que le professionnel de soins doit avoir clairement et préalablement informé le patient au sujet des soins envisagés. **L'information porte sur le but, la nature, le degré d'urgence, la durée, la fréquence, les évolutions, les contre-indications, les effets secondaires, les risques, les alternatives, le coût**. En situation d'urgence et si le patient est incapable de donner son consentement, le prestataire de soins agit dans l'intérêt de la santé du patient.
- Droit à **retirer son consentement** avec information préalable des conséquences impliquées par ce choix. Le professionnel de soins a l'obligation de respecter ce refus.
- Droit à avoir un **dossier tenu à jour**, à pouvoir le **consulter** et à en obtenir une **copie sous forme papier ou électronique**. La première copie est gratuite. Ce dossier contient les **données personnelles** suivantes : l'identité du patient, les informations relatives aux soins (examens, diagnostics, chronologie des soins dispensés, etc.). Le patient a le droit de demander le **transfert** de son dossier vers un nouveau prestataire de soins. Il a également le droit de **recevoir des explications sur le contenu de son dossier**.
- Droit au **respect de son intimité** et à la **protection de sa vie privée**. Le patient a le droit de demander la présence d'une **personne de confiance**. Il peut s'agir d'un membre de la famille, d'un ami, d'une connaissance ou de toute autre personne désignée par lui. Cette personne de confiance peut exercer tous les droits du patient que celui-ci lui accorde. Elle peut agir en l'absence du patient mais à la demande de ce dernier ; dans ce cadre, elle a uniquement le droit d'être informée sur l'état de santé du patient, sur une intervention de soins envisagée et le droit de consulter le dossier du patient.
- Droit à introduire une **plainte** auprès d'un service de médiation.
- Au cas où le patient n'est pas en mesure d'exercer lui-même ses droits, la totalité de ceux-ci peuvent être exercés par un **représentant**, choisi par le patient ou désigné. Les règles de désignation diffèrent selon que le patient a atteint ou pas l'âge de la majorité.

En 2022, la Commission fédérale relative aux droits du patient soulignait la nécessité d'envisager, pour ce cadre réglementaire, « *les développements technologiques survenus depuis 2002 et anticiper autant que*

possible *les évolutions qui pourraient survenir dans ce domaine* » ([avis 2024-04-18](#)).

Que dispose en définitive le cadre réglementaire ?

Le cadre est touffu et les balises, nombreuses. Plusieurs textes ont pour objet d'alerter sur les **dangers encourus par les droits humains au vu du développement de l'intelligence artificielle** et tendent à protéger ces droits. Toutefois aucun de ces textes n'est contraignant et leurs dispositions s'apparentent davantage à de **beaux principes peu ancrés dans la réalité**. Le fait qu'aucun des 46 pays que compte le Conseil de l'Europe n'ait ratifié la *Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'Etat de droit*, empêchant *ipso facto* son entrée en vigueur, en est une preuve éloquente et inquiétante. Du côté des législations contraignantes, la plupart sont techniques comme l'AI-Act et la loi NIS2. Le RGPD et la loi anti-discrimination, censés structurer les possibles recours pour violation des droits humains dans le cadre de l'utilisation de l'intelligence artificielle, paraissent des **garde-fous bien faibles**, l'un parce qu'il est sous le coup d'une révision prochaine qui en réduira la portée et l'autre car les dédommagements qu'elle prévoit sont très limités alors que les préjudices subis en matière de santé peuvent être très importants. Enfin, **la loi qui définit et protège les droits du patient**, parce qu'elle n'envisage pas les évolutions technologiques que connaît actuellement le secteur médical, et notamment la montée en puissance de l'intelligence artificielle, apparaît datée, peu adaptée au nouveau contexte de la « médecine augmentée » et **demanderait à être revue**.

Restent les principes cardinaux de la Constitution belge comme socle des droits :

- **Egalité** : tous les Belges sont égaux devant la loi (article 10)
- **Non-discrimination** : La jouissance des droits et libertés reconnus aux Belges doit être assurée sans discrimination (article 11)
- **Respect de la vie privée** (article 22)
- **Inclusion** : chaque personne en situation de handicap a le droit à une pleine inclusion dans la société, y compris le droit à des aménagements raisonnables (article 22 ter)
- **Droit à la dignité, à la protection de la santé et à l'aide médicale** (article 23)

4/ L'intelligence artificielle en soins de santé : impacts et enjeux

L'IA en soins de santé : des enjeux différents suivant les acteurs

Producteurs, acheteurs, médecins, patients, tous sont concernés par l'implémentation en cours de l'IA en soins de santé. Mais **les enjeux diffèrent** selon que l'on appartient à l'une ou l'autre de ces catégories :

- Les préoccupations des **producteurs** de systèmes d'IA vont à la **réglementation** afin de la comprendre et de la respecter.
- Les **patients**, pour leur part, veulent **comprendre** leur situation de santé et son évolution probable, les traitements proposés, etc. et, en l'absence d'information, font généralement **confiance aux médecins** par défaut.
- Les **prestataires de soins** sont préoccupés par la question de leur **responsabilité** en cas d'application d'une décision d'IA et sont peut-être tentés de faire **confiance aux certifications** existantes des outils utilisés.
- Les **acheteurs** d'IA sont quant à eux confrontés à la **pression sur le financement des soins de santé** et tentés, voire obligés, de réduire les coûts.

La place centrale du « standard of care » et la question de la responsabilité du prestataire de soins

Que se passe-t-il, avec l'implémentation de l'IA, en cas de prise de décision médicale automatisée et quelle est alors la responsabilité du prestataire de soins ? **En Europe, le médecin reste le responsable final des décisions médicales.**

Lorsqu'un problème se pose dans la prise en charge d'un patient, on se réfère au « standard of care » ou

« norme de soins ». On peut imaginer qu'à l'avenir, les systèmes d'IA automatisés deviendront de plus en plus LA « norme de soins ». Le médecin ne serait alors pas responsable d'une erreur médicale due à l'IA si la décision du système d'IA en vient à correspondre à la « norme de soins ». Le danger de la responsabilité, en cas d'erreur médicale due à l'IA, à condition que le médecin soit capable d'utiliser les systèmes d'IA, s'estomperait peu à peu, mais pas pour les médecins peu aguerris en matière de systèmes automatisés qui n'y recourraient pas. Par ailleurs, que le médecin soit considéré responsable ou pas d'une erreur médicale, l'impact pour le patient d'une telle erreur demeure et la peur de l'erreur pourrait affecter la relation de confiance entre le patient et son prestataire de soins. Pour le bien de tous, prestataires ET patients, **il est crucial dès lors que tout médecin ou équipe d'accompagnement médicale et paramédicale dispose de compétences suffisantes en IA, que la norme de soin coïncide ou non avec celle-ci, afin d'être capable de discerner et de critiquer le bien-fondé des décisions prises par une IA.** Cette exigence concerne également les personnes auxquelles certains actes de soins ou d'accompagnement, qui embarqueraient l'IA, seraient délégués (dans les hôpitaux, institutions, maisons de retraite et de soin, à domicile).

Cette nécessité se retrouve dans l'AI-Act, qui prévoit l'obligation pour les organisations de développer les compétences de leurs travailleurs qui utilisent l'IA. Mais qu'en est-il sur le terrain ? Le risque est que se développe une **médecine à deux vitesses**, entre professionnels compétents en IA et ceux qui ne le sont pas, entre hôpitaux qui disposent d'outils IA et d'autres qui en sont dépourvus, **en contradiction avec le droit du patient** à bénéficier d'une prestation de soins de qualité, à savoir des **meilleurs soins possibles en fonction des connaissances médicales et des technologies disponibles**. Avec, éventuellement, le risque supplémentaire de creuser les **inégalités entre les patients capables de se payer une médecine de pointe, plus chère, et les autres.**

L'enjeu de la relation prestataire/patient ou la question de la confiance

Pour que les soins de santé qui embarquent l'IA puissent susciter la confiance, plusieurs critères doivent être rencontrés :

- La qualité du développement des systèmes d'IA appliqués à la médecine
- La gestion des biais
- La formation en IA des professionnels de la santé

1°) La qualité du développement des systèmes d'IA appliqués à la médecine

L'AI-Act impose aux fournisseurs de systèmes d'IA l'obligation de fournir des chiffres sur la performance du dispositif commercialisé. Mais il n'est pas nécessaire de donner des précisions sur la qualité et la rigueur méthodologiques avec lesquelles le système d'IA a été développé : comment la performance est-elle atteinte ? quel a été l'échantillon pris en compte ? sa taille ? quelle méthode a été suivie ? comment la performance a-t-elle été testée pour sa validation ? le modèle a-t-il été critiqué ? L'AI-Act est une législation pour les produits et la médecine n'en est pas un. **La documentation prescrite par l'AI-Act ne répond pas aux standards scientifiques de la médecine.** En effet, une machine est valable, qu'elle soit déployée en Finlande ou en Espagne. Mais, en médecine, les individus changent d'un lieu à l'autre. Pour que le dispositif médical soit performant, il faut qu'il se soit développé au départ de populations diversifiées, hétérogènes. Ainsi, par exemple, si on a pris un hôpital, entraîné le dispositif sur une première moitié de patients et testé avec la deuxième moitié du même hôpital, les chiffres de performance seront excellents, mais le dispositif sera de piètre qualité car toutes les données viennent de la même population.

Par ailleurs, le développement des IA médicales est aux mains des entreprises. Dans le meilleur des cas, **les médecins interviennent dans le processus d'élaboration des dispositifs à titre de consultants ponctuels.** Les modèles développés par les universités ou des collectifs se comptent sur les doigts d'une main. Donc, les modèles sont essentiellement commerciaux. De plus, **la médecine générale et les pathologies rares sont exclues d'emblée des développements** : la première, parce que les généralistes n'ont pas les moyens d'investir dans ce genre d'outils ; les deuxièmes, parce qu'elles ne sont pas rentables.

Tous ces éléments ont une influence préoccupante sur la qualité des dispositifs d'IA utilisés en soins de santé et peuvent porter atteinte à la relation de confiance entre le patient, son prestataire de soins et les

outils utilisés par ce dernier.

2°) La gestion des biais

Actuellement, tous les hôpitaux belges disposent d'au moins un algorithme avec une finalité propre, qu'elle soit médicale (radiologie, insuffisance cardiaque, gastroentérologie par exemple) ou administrative (logique hospitalière, pharmacie par exemple). La création d'un algorithme n'est pas neutre. Tout d'abord, parce que cela implique la traduction d'une règle en code source. Cette traduction n'est pas immédiate, elle suppose des choix et des **décisions concernant notamment les critères d'application de la règle algorithmique**. Ensuite, les algorithmes apprenants vont être entraînés au départ d'un **jeu de données**. Celui-ci fait également l'objet d'un **choix** et celui-ci peut être **plus ou moins représentatif des populations-cibles**. Ces choix ont un impact sur la qualité de l'algorithme développé.

Il convient dès lors de distinguer **deux types de biais** : les biais algorithmiques *a posteriori*, qui permettent de personnaliser le soin, en fonction par exemple du handicap, de l'âge, de telle ou telle pathologie, et les biais *a priori*, ceux résultant des choix de développement. Si les premiers peuvent être utiles, et même bénéfiques, au patient, à condition d'y inclure aussi le contexte spécifique du patient, il n'en va pas de même des seconds. Ces derniers peuvent avoir pour conséquence d'**exclure** des groupes de personnes, ayant certaines pathologies par exemple, avec des conséquences sur **l'adéquation des prestations de santé** qui seront octroyées à ces bénéficiaires. Dans ce cas, le médecin doit avoir la formation et l'information suffisantes pour rester critique face à l'outil d'IA qu'il utilise, être capable de repérer les biais de développement, de détecter à qui peut s'appliquer l'outil et, éventuellement, de choisir de ne pas suivre les suggestions de l'IA.

La discrimination algorithmique a en outre des répercussions sur les droits du patient. Pour donner son « **consentement éclairé** » à une prestation de soins ou à un traitement, le patient doit pouvoir faire confiance aux propositions qu'on lui soumet. Mais comment sait-on qu'on est victime de discrimination algorithmique ? Le patient se situe dans une position asymétrique de connaissances et de pouvoir par rapport à un prestataire recourant à de tels outils. Certes, on peut alléguer que c'était déjà le cas dans la médecine d'avant l'IA : à moins d'être médecin ou d'en avoir dans son entourage proche, le patient est rarement en position de pouvoir réfléchir au bien-fondé de tel ou tel traitement. Il fait confiance par défaut à son prestataire de soins. Mais l'IA ajoute une couche d'**opacité lorsque le médecin lui-même n'est pas en mesure de rester critique face à la proposition de l'IA et d'envisager, éventuellement, de ne pas la suivre**. Or c'est bien ainsi que se profile la médecine de demain : une médecine augmentée par la puissance de l'IA. Elle nécessite des professionnels du soin capables de comprendre l'IA et de la contrôler, sous peine que la relation de soins se résume, après-demain, à un face à face patient/IA, dont le médecin ne serait plus que l'interface.

3°) La formation en IA des professionnels de la santé

La formation des professionnels de la santé en matière d'IA, on le voit, est cruciale, aussi bien pour les patients que les prestataires de soins :

- une **formation solide, en profondeur et continue** permettant aux professionnels de la santé de rester critiques face aux suggestions de l'IA, d'évaluer le bien-fondé de ces suggestions, de les expliquer ensuite au patient de manière claire et compréhensible afin de garantir à ce patient le droit à un consentement éclairé
- une **formation accessible** non seulement aux jeunes prestataires fraîchement diplômés, mais aussi à ceux qui sont déjà en exercice
- avec une **adaptation de la déontologie**, incluant le libre-arbitre du médecin face aux suggestions de l'IA dans l'intérêt supérieur du patient

Seule une telle formation permettra :

- d'intégrer les bienfaits de l'IA dans une médecine « augmentée »
- de lutter contre les erreurs médicales, une médecine à deux vitesses, une médecine de pointe accessible seulement aux plus fortunés

- de garantir le plein exercice des droits du patient
- de maintenir le standard européen d'une relation de soins d'humain à humain

En Belgique, contrairement à d'autres pays européens, il n'y a pas de formation continue obligatoire.

L'enjeu de la littératie en soins de santé ou le besoin de comprendre

Par « littératie en soins de santé », on entend les « *connaissances, motivations et compétences permettant d'accéder à de l'information dans le domaine de la santé, la comprendre, l'évaluer et l'appliquer. Ces connaissances, motivations et compétences permettent de se forger un jugement et de prendre une décision en matière de soins de santé, de prévention et de promotion de la santé, dans le but de maintenir et promouvoir sa qualité de vie tout au long de son existence* » ([Définition de la Fondation Roi Baudouin](#)). La littératie en soins de santé se définit au carrefour de l'individu et du système des soins de santé, au point de rencontre entre les compétences de l'individu et les exigences du système. Du côté des compétences individuelles influençant la littératie en soins de santé, on trouve :

- Les capacités cognitives (mémoire, raisonnement, résolution de problèmes) et la maîtrise de la langue
- Le réseau social comme première source d'information
- Les compétences psychosociales (s'informer, demander, etc.)
- Le registre culturel (les représentations, les valeurs, les croyances, etc.)
- Les conditions de vie (revenus, instruction, travail, etc.)
- Les caractéristiques individuelles (âge, déficiences, etc.)

Les facteurs inhérents au système de soins de santé, d'autre part, sont :

- Les systèmes et moyens d'information (qualité, quantité, disponibilité, etc.)
- Le système de santé et la protection sociale (conditions d'accès, complexité, etc.)
- Les interactions avec le système (exemple : réduction des guichets physiques)

En Belgique, d'après la Fondation Roi Baudouin, **80% des patients ignorent ce qu'est une « donnée de santé »** ([Définition de la Fondation Roi Baudouin](#)). De plus, **un tiers de la population a un faible niveau de littératie**, c'est-à-dire que ces personnes relèvent des niveaux 1 et 2 (**inadéquat et problématique**) sur une échelle qui en compte 4. Or, accéder à l'information, comprendre, juger de la fiabilité et de la pertinence sont des compétences **nécessaires pour pouvoir exercer ses droits en tant que patient** et opérer ses propres choix en matière de santé, y compris des choix qui ne seraient pas ceux prônés par le prestataire de soin.

Les situations à risque, qui mettent en péril la littératie en soins de santé, sont :

- L'éloignement de l'information
- L'absence de réseau d'information
- La fracture numérique
- La perte de confiance vis-à-vis de l'information

Il en résulte que l'émergence d'une médecine augmentée par l'intelligence artificielle impacte significativement une littératie en soins de santé déjà faible en Belgique. En effet, **en modifiant le système des soins de santé, elle accentue les situations à risques** : elle augmente l'opacité de l'information, elle amoindrit les compétences du réseau proche en réduisant le nombre de ceux qui peuvent fournir des explications, elle active la fracture numérique et met en danger la relation de confiance entre le patient et le prestataire de soins.

A ceci s'ajoute le fait que **les dispositifs d'IA ne sont pas toujours explicables**, indépendamment des capacités du patient à comprendre et de la volonté du praticien à expliquer. En effet, certaines études montrent que les dispositifs les plus explicables ne sont pas les plus performants. Le principe d'explicabilité, cher à l'AI-Act, et la performance ne vont pas forcément de pair tant l'output médical dérive de systèmes complexes. Qu'en est-il alors, dans ce contexte, du droit du patient à recevoir des explications et à être éclairé dans les décisions qu'il doit prendre concernant sa santé ?

Pour le dire brièvement, **l'intelligence artificielle rend la littératie en soins de santé des Belges encore plus inadéquate qu'elle ne l'était déjà et, par voie de conséquence, met en péril les droits du patient.**

L'enjeu des financements ou la question des moyens

En Belgique, les financements possibles pour le développement d'IA en soins de santé sont à la fois publics et privés.

Du côté des pouvoirs publics, les financements sont octroyés via des **appels à projets**. Avec la conséquence que ces projets sont **éparpillés**. Le fait que la santé relève de différents niveaux de pouvoir en Belgique renforce encore cet éparpillement. Il n'y a donc pas de projet structurant pour l'ensemble de la Belgique. Ensuite, toutes les aides aux entreprises qui font de la tech vont à des **modèles d'IA payants, privés, fermés**. L'IA est par conséquent aux mains d'**intérêts financiers et commerciaux**. Et nul ne sait si les projets-pilotes, ainsi lancés, pourront se poursuivre, ce qui hypothèque la **continuité des parcours de soins basés sur l'IA**.

Du côté du privé, le secteur pharmaceutique est un acteur important dans le développement de la santé digitale. En effet, l'industrie pharmaceutique est intéressée par les données qui se trouvent à l'hôpital. Et l'hôpital, pour sa part, cherche à s'outiller en dispositifs d'IA médicaux. De là naît une **collaboration qui va permettre de satisfaire les deux parties** : l'industrie pharmaceutique propose un financement à l'hôpital pour une solution IA qui permettra de mieux soigner les patients et qui passera par la collecte des données au profit de la firme pharmaceutique. Mais que se passe-t-il après ? Lorsque la firme pharmaceutique possède les données dont elle a besoin, **le financement s'interrompt**. A charge de l'hôpital de continuer à financer l'outil ou d'interrompre le processus de soins. Ce système joue **au détriment du patient** qui là aussi aura bénéficié un temps d'un trajet de soins ultraperformant, lequel aura éventuellement amélioré sa qualité de vie mais qui s'interrompra faute de financements disponibles pour se poursuivre.

La situation des hôpitaux face au développement d'une « médecine augmentée » est en effet **financièrement tendue**. Les obligations en matière d'IA qui s'appliquent à eux sont multiples : tenir à jour un registre d'IA, évaluer et gérer les risques, mettre en conformité, former le personnel, assurer un suivi et soumettre les systèmes d'IA à des audits. De nouvelles fonctions doivent être implémentées : les hôpitaux doivent se doter d'un *Data Protection Officer* (DPO) et d'un *Chief Information Security Officer* (CISO). **La charge contraignante augmente et ne fait l'objet d'aucun financement supplémentaire**. A terme, la **commercialisation à grande échelle** par les hôpitaux des données de santé des patients pourrait devenir une solution très tentante. Quoi qu'il en soit, **la relation de soin n'est désormais plus bilatérale, il y a dorénavant 3 partenaires en présence : le prestataire de soin, le patient et l'entreprise commerciale** qui a accès aux données de santé et à l'évolution de santé des patients. Cette nouvelle configuration de la relation de soin **altère l'esprit de la loi du 6 février 2024 sur les droits du patient** visant à instaurer une relation de collaboration et de dialogue entre patient et soignant.

Plus généralement, l'organisation du développement des IA médicales en Belgique interpelle. D'une part, des financements publics, c'est-à-dire l'argent du citoyen, sont accordés, à hauteur de millions d'euros, à des entreprises pour développer **des solutions qui seront ensuite payées par le patient**. D'autre part, **les données de santé collectées auprès du patient ont une valeur monétaire**, parfois exorbitante parce que la valeur que l'on peut générer avec ces données est énorme. En définitive, **le citoyen paie trois fois des systèmes de soin : avec ses données, avec ses impôts et avec ses deniers propres** lorsqu'il devient patient du processus de soin.

L'enjeu de la gestion des données ou le besoin de sécurité

Les **banques de données à caractère personnel** sont rangées dans les « **risques élevés** » par l'AI-Act. Elles sont donc **soumises aux obligations**

- de précision, robustesse et sécurité ;
- d'identification et de gestion des risques ;
- d'analyse d'impact sur les droits humains ;
- de documentation technique et de gestion documentée de la qualité ;
- d'évaluation de conformité et d'enregistrement dans la Banque de données centrale de la Commission Européenne (voir ci-dessus, le point consacré à l'AI-Act).

Dans les hôpitaux, la gestion des données de santé relève en outre du **RGPD** : les données doivent être anonymisées (suppression des données personnelles) ou pseudonymisées (remplacement des identifiants

par des pseudonymes) avant d'être introduites dans des IA générales et le patient peut retirer son **consentement** à tout moment.

Tout cela semble très rassurant. Oui, mais...

- Où les données sont-elles conservées ? Sur des serveurs ou dans le cloud. Le cloud protège des pannes mais est davantage **exposé aux cyberattaques** et engendre une **préoccupation supérieure pour la cybersécurité**. Tous les hôpitaux belges ne recourent pas au cloud et certains de ceux qui en étaient partisans sont d'ailleurs en train de rapatrier leurs données sur des serveurs internes.
- Dans le cas des **maladies rares**, l'anonymisation n'est pas garantie.
- En mars 2025, l'entrée en vigueur du [règlement 2025/327 sur l'espace européen des données de santé](#) (EHDS ou *European Health Data Space*) a instauré le partage sans limite des données médicales. Différentes phases sont mises en place pour une application progressive de ce règlement.
 - En **2029**, les prestataires de soins seront tenus **d'échanger les résumés électroniques** des patients, les **prescriptions** et les **dispensations** dans un format standardisé, conforme aux normes européennes.
 - En **2031**, tous les systèmes de dossiers médicaux électroniques couverts par l'EHDS devront être pleinement certifiés, garantissant une **interopérabilité** renforcée.
 - À plus long terme, en **2034**, des connexions avec des **pays tiers** seront établies.

Sur la base de ce règlement, les données médicales deviennent exploitables dans d'autres pays européens que celui de leur origine pour des soins au patient concerné (utilisation primaire des données). Elles sont également **utilisables à des fins de recherches et d'innovation**, et notamment **pour l'entraînement des IA** (utilisation secondaire des données). Face à l'espace européen des données de santé, les droits du patient en sortent amoindris. En effet, **le consentement des patients est considéré acquis par défaut**. Si le patient veut s'y opposer ou choisir à quoi ses données peuvent être utilisées, il peut le faire mais doit lui-même initier la démarche. On le voit, **les droits du patient sont devenus conditionnels** car conditionnés pour le patient à être informé, à être capable de rechercher la procédure adéquate pour éventuellement s'opposer et à prendre le temps d'entamer les démarches nécessaires. De surcroît, **le droit d'accès sans limites aux données médicales des citoyens européens n'est assorti d'aucun devoir** pour les gestionnaires de données, les professionnels de la santé, les développeurs d'IA et les Etats auxquels ces différents acteurs appartiennent. C'est d'ailleurs la raison pour laquelle des patients, des associations de psychologues et la Ligue des Droits Humains ont introduit, le 17 février 2025, un **recours au Conseil d'Etat** contre les arrêtés royaux transposant pour la Belgique le règlement européen : ils dénoncent une **atteinte au secret médical et au droit du consentement libre et éclairé**.

Car, en définitive, la question qui se pose est la suivante : **le patient est-il encore propriétaire de ses données personnelles à caractère médical et maître d'en disposer librement ?**

Cette ouverture de l'espace européen des données de santé pourrait en outre être utilisée, **dans l'avenir**, à d'autres fins que celles prévues actuellement. Des acteurs privés pourraient être tentés d'en demander l'accès pour obtenir des informations de santé sur leurs clients invoquant un « **intérêt légitime** », comme les assurances ou les banques par exemple. Il est inquiétant que **les données sensibles des citoyens ne soient protégées que par les valeurs et convictions politiques des dirigeants du moment**.

5/ Concrètement, l'IA dans les trajets de soins

Au cours des dernières années, l'avènement de l'intelligence artificielle a gagné la réalité concrète des trajets en soins de santé. Le recours à l'IA dans les traitements implique tout à la fois des avantages et des inconvénients : d'une part, l'IA génère des avancées médicales au bénéfice du patient ; d'autre part, elle génère également des risques inédits.

D'après la *Vlaams patiëntenplatform*, les plus-values de l'IA dans les soins de santé sont les suivantes :

- **Les diagnostics** : ils acquièrent une **grande précision** et une **grande efficacité** grâce à la capacité d'analyse des systèmes d'IA appliquée aux données médicales, comme les images médicales ou les résultats de laboratoire.

- Les systèmes d'IA sont également capables de **prédire des maladies à partir des données des patients**.
- **Traitements** : grâce à l'IA, il est possible de **personnaliser** les traitements, en tenant compte des antécédents médicaux, du profil génétique, d'allergies à certains médicaments, par exemple, qui caractérisent tel patient à la différence de tel autre. Grâce à la limitation des effets secondaires et à l'optimisation des résultats, **l'état du patient et sa qualité de vie s'améliorent**.
- **Dépistage, prévention et santé publique** : les capacités d'analyse de l'IA ne s'appliquent pas seulement à des individus mais aussi à des ensembles de patients, permettant de détecter des **signaux d'alarme** et de prédire des risques pour la santé collective, comme les épidémies par exemple. Ces données, à leur tour, nourrissent les **politiques de prévention et de santé publique**.
- **L'automatisation des tâches administratives** comme la planification des rendez-vous ou la gestion des données des patients libère du **temps à consacrer à l'accueil et au suivi humain**.

L'essor de l'intelligence artificielle et ses progrès rapides suscitent un grand espoir, particulièrement auprès des patients pris dans de longs trajets de soins, voire des trajets à vie, comme les personnes en situation de handicap. Toutefois, l'engouement pour cette « médecine augmentée » ne doit pas faire perdre de vue les risques qu'elle comporte. La *Vlaams patiëntenplatform* en répertorie de quatre types :

- **Erreurs** : malgré le potentiel quasi magique qu'on lui prête, l'IA est faillible et peut commettre des erreurs. Dans le domaine de la santé, ces erreurs peuvent avoir **un impact et des conséquences très sérieux sur la santé du patient et sa qualité de vie**.
- **Biais** : l'IA est basée sur un traitement des données. **Ces données doivent être de qualité et nécessitent une mise à jour régulière et une supervision constante sous peine de générer des erreurs**, qui peuvent à leur tour être sources erreurs médicales plus ou moins lourdes pour le patient.
- **Sécurité des données et vie privée** : dans le domaine des soins de santé, les systèmes d'IA manient des **données sensibles**. Les récolter peut supposer des **intrusions plus ou moins sérieuses dans la vie privée** des patients. Il est crucial de **mesurer l'atteinte à la vie privée au regard des bénéfices attendus et d'assurer la sécurité de ces données** afin de les protéger d'intentions malveillantes comme les cyberattaques.
- **Une trop grande dépendance vis-à-vis des outils d'IA**, enfin, pourrait, à terme, réduire les capacités des professionnels de la santé dans les domaines et les compétences confiés à l'IA. Il est impératif que les professionnels de la santé restent capables d'**analyser** et de **critiquer**, voire de **rejeter**, les résultats obtenus par l'intervention de l'IA.

Pour la *Vlaams patiëntenplatform*, le recours de l'IA dans les trajets de santé expose le secteur médical à de solides défis pour l'avenir. Ses recommandations sont les suivantes :

- Il est nécessaire de **réglementer** l'usage de l'IA dans les soins de santé afin de garantir une application sûre et éthique ;
- Il est également crucial d'assurer une **information claire et accessible aux patients**, surtout lorsqu'il s'agit de décisions sensibles concernant leur santé ;
- La **formation des prestataires de soins en matière d'IA** doit être un prérequis obligé pour tout usage d'un système d'IA dans le domaine de la santé ;
- Enfin, il est indispensable de **clarifier la notion de responsabilité** lors de prise de décision médicale avec intervention de l'IA.

6/ Conclusions et recommandations

Conclusion

Force est de constater, en tout premier lieu, que l'intégration de l'IA aux soins de santé ravive les préoccupations et remobilise les recommandations que le CSNPH énonçait déjà dans sa note de position de 2017 consacrée au secteur de la santé. Parmi ces préoccupations, citons notamment :

- Le **déséquilibre de connaissances** entre le patient et le prestataire de soins
- Ce déséquilibre peut aboutir à des parcours de soins imposés, qui ne respectent pas les **choix**, et singulièrement les choix de vie, du patient
- La tentation, pour le prestataire, de **se focaliser sur les aspects de surveillance et de soins** en oubliant

les questions essentielles d'une part de la qualité de vie du patient et de ses aidants proches, et d'autre part de l'implication de ces derniers dans les décisions de soin (*shared decision making*)

Dans sa note, le CSNPH recommandait entre autres de :

- Veiller à la **continuité des soins**
- Respecter la **liberté de faire ses propres choix**
- Assurer une **information suffisante, accessible et de qualité** durant tout le parcours de soin
- Veiller à l'**accessibilité financière** des soins
- Considérer le patient comme **acteur de sa santé et interlocuteur des prestataires de soins** ; celui-ci n'est **pas un consommateur** de soins qui devrait s'adapter à l'offre mais une personne à accompagner au mieux dans sa demande médicale spécifique
- Sensibiliser les prestataires de santé aux **droits humains**

Ces préoccupations et recommandations acquièrent une acuité accrue dans un contexte de « médecine augmentée » par l'IA.

Au-delà des points singuliers qui ont été analysés précédemment et rappelés ci-dessus, qui méritent tous une grande attention, le CSNPH constate avec préoccupation une **érosion des protections des droits individuels au profit d'intérêts présentés comme collectifs** – l'amélioration de la qualité des soins de santé – qui se déclinent toutefois en intérêts indéniablement privés.

- Le **prix à payer** pour l'implémentation innovante de techniques médicales avancées **repose sur l'individu**, citoyen et patient à l'occasion. Celui-ci finance le développement de ces innovations avec ses données et ses impôts et payera avec ses deniers la possibilité d'en bénéficier en tant que patient.
- Le coût de l'innovation n'est pas seulement financier. Il comporte de surcroît un **recul des droits individuels** :
 - L'opacité des systèmes d'IA pour les patients ET pour les médecins rend malaisé l'exercice du **droit au consentement éclairé** et met à mal la **relation de confiance** entre prestataire de soin et patient.
 - Le droit de **s'opposer au traitement de ses données à caractère personnel et aux décisions automatisées** est restreint par l'entrée en vigueur de l'espace européen des données médicales : le consentement du patient est acquis par défaut et la possibilité de s'y opposer est entièrement à charge de l'individu. Alors que, parallèlement, le droit d'accès aux données médicales des citoyens européens n'est assorti d'aucun devoir en contrepartie.
 - L'AI-Act ne prévoit **pas de procédure individuelle de plainte ou de recours** pour les individus qui s'estimeraient victimes d'une **violation de leurs droits fondamentaux**. Plaintes et recours devront se faire sur la base d'autres réglementations, RGPD et anti-discrimination essentiellement. En Europe, **le RGPD est remis en question** et, de manière générale, **la complexité des algorithmes rend les discriminations difficiles à détecter**. L'**aspect transnational** de l'IA ne facilite pas non plus ces recours, déjà malmenés : comment fait-on pour introduire une plainte contre un dispositif d'IA conçu dans la *Silicon Valley* ?
 - Les organismes nationaux qui protègent les droits humains fondamentaux ont, dans le cadre de l'AI-Act, un **rôle purement consultatif** et **ne peuvent pas agir au nom des individus**.

IA et algorithmes entraînent donc à la fois une asymétrie de pouvoir et de connaissances, au détriment de l'individu, mais de surcroît une asymétrie dans l'exercice des droits et des devoirs.

Tout se passe comme si, face à des intérêts collectifs – l'innovation, l'amélioration des soins de santé, la santé publique –, présentés comme supérieurs, les droits individuels devaient s'incliner et accepter de se restreindre. Les propositions de révision du RGPD actuellement contenues dans le Digital Omnibus de la Commission Européenne s'inscrivent dans cette même logique de réduction des droits fondamentaux. A cela s'ajoute que la « **collectivisation** » du bien commun entraîne également un **affaiblissement des droits**. En effet, comme le faisait remarquer le Comité Ad Hoc Artificial Intelligence du Conseil de l'Europe ([CAHA](#)), « **notre arsenal réglementaire, s'il est bien armé contre les risques que nous avons appelés individuels, l'est**

bien moins par rapport [aux] risques collectifs⁸ ». Or l'intelligence artificielle engendre non seulement des risques pour les individus, leurs droits et leurs libertés, mais également pour des groupes d'individus : « **les discriminations que peuvent engendrer les techniques d'intelligence artificielle mettent en jeu au-delà des personnes des groupes d'individus** réunis par le genre, la race mais également par la présence d'une donnée génétique qui permet de prédire la maladie future [...]»⁹ ». Mais qu'est-ce qu'une « discrimination collective » ? A partir de quand y a-t-il « discrimination collective » : quand 20% des personnes du groupe en question sont discriminées ? 50% ? 80% ? 100% ? Ces notions et enjeux ne sont pas traduits dans le droit. Dès lors, **affaiblir les droits individuels au nom d'une collectivisation des intérêts et des enjeux, c'est laisser le citoyen doublement sans protection face aux risques encourus, qu'ils soient individuels ou collectifs.**

Recommandations

De manière générale, le CSNPH demande instamment aux décideurs politiques de défendre des exigences fortes en matière de droits humains dans le cadre des discussions relatives au Digital Omnibus de la Commission Européenne, en particulier en ce qui concerne la révision de l'AI-Act, du RGPD et la directive NIS2. Il convient de renforcer, et non d'amoindrir, les droits des citoyens face à la déferlante de l'intelligence artificielle.

Le CSNPH est par ailleurs conscient du cadre juridique dans lequel s'inscrit le recours à l'IA dans les soins de santé et, en particulier, de l'harmonisation maximale à laquelle sont soumis les Etats par l'AI-Act. Toutefois, le CSNPH, dans le cadre de ses compétences, estime essentiel d'insister sur certains points d'attention cruciaux et de recommander ce qui suit :

Concernant le cadre et les obligations générales :

- Ratification de la Convention du Conseil de l'Europe et mise en place de ses principes au niveau national
- Appliquer les recommandations du Conseil des Ministres du Conseil de l'Europe aux Etats Membres sur les impacts des systèmes algorithmiques sur les droits humains du 8 avril 2020
- Remplacer le consentement par défaut par le droit au consentement éclairé explicite dans le cadre de l'espace européen des données de santé
- Appliquer les principes de la Déclaration des droits numériques et notamment interdire les systèmes d'IA qui « préjugent des choix des personnes » en violation du droit de l'Union
- Prévoir une Charte de valeurs et de fonctionnement "IA et personnes en situation de handicap" au niveau des décideurs politiques, acteurs économiques, centres de soins et d'accompagnement de personnes en situation de handicap
- Vraie protection des droits du citoyen et possibilité de recours
- Définir la « discrimination collective » et se donner des outils pour lutter contre cette forme de discrimination
- Renforcer le RGPD et s'assurer qu'il est bien respecté
- Augmenter le délai de conservation des données de traçage // avis Cour Européenne de Justice
- Réguler les IA à risques modérés par des mesures contraignantes
- Créer un cadre juridique spécifique pour les systèmes d'aide à la décision médicale car ces systèmes brassent une très grande quantité de données
- Compléter la législation produit de l'AI-Act par des contraintes spécifiques pour les IA en soins de santé, notamment pour la documentation fournie par le producteur (obligation de fournir des

⁸ Yves POULLET, ancien recteur de l'Université de Namur et directeur du Centre de recherches informatiques et droit (CRID) : [Poullet, Y., « À propos de quelques documents internationaux relatifs à l'éthique de l'intelligence artific... - Strada lex](#)

⁹ Idem.

- informations complètes et accessibles sur la méthodologie de développement et de validation)
- Garantir la supervision humaine des dispositifs d'IA
- Prévoir des garanties pour anonymisation des données de santé
- AI-Act : avoir un bon produit ne suffit pas. Cela implique des coûts s'il est nécessaire de remédier à des impacts sociétaux
- Devoirs en contrepartie des droits d'accès aux données médicales européennes
- Mieux encadrer l'interdiction de toute commercialisation des données de santé
- Développer un droit du numérique afin d'encadrer son développement : avec protection des droits humains et des droits du patient
- Etendre évaluation des conséquences d'un outil : pas seulement sur les droits humains, mais aussi sur RGPD/vie privée, droits du patient, impact environnemental
- Traçage individuel des données afin de pouvoir comprendre en temps réel quelles données personnelles sont utilisées, pour quoi faire, identifier les erreurs et dénoncer les abus éventuels
- [Masanté.be](https://www.masante.be) : y inclure toutes les données qui intéressent le citoyen, où il puisse exercer ses droits
- Obligation d'informer le citoyen lorsqu'une décision individuelle a été prise le concernant impliquant un algorithme ou une IA
- Articuler l'article 9 de l'AI-Act (définition du niveau acceptable de risque résiduaire) et l'article 35 du RGPD (risque élevé sur droits et libertés des personnes physiques) pour instaurer l'obligation
 - o 1) d'évaluer l'impact sur la protection des données et aussi sur les droits et libertés des personnes physiques,
 - o 2) d'évaluer les risques et les incidents au regard des droits fondamentaux,
 - o 3) de fournir de l'information sur la gouvernance des données (critères de sélection des données et documentation des capacités d'enregistrement de l'IA),
 - o 4) de tester les données et l'exactitude des outputs,
 - o 5) de mettre en place des mesures de surveillance humaine.
- Chatbots : mettre en place des garanties de transparence, de fonctionnement, d'équité et de lutte contre les discriminations, ainsi que des mesures pour limiter les risques des « compagnons thérapeutiques » sur la santé
- Organiser un débat démocratique public et éclairé sur l'usage des algorithmes et des IA et le faire aboutir en des textes de lois clairs et concrets pour améliorer l'accompagnement des patients
- Introduire la possibilité, garantie par la loi, d'introduire une plainte avec présomption de discrimination, avec compensations financières et individuelles
- Protéger les standards de soins européens avec un contact en chair et en os avec le prestataire de soins
- Reprise de *IA for Health* avec financement approprié et mandat politique clair
- Imposer une analyse de risques préalable au déploiement d'un dispositif d'IA, qui considère ledit dispositif tour à tour du point de vue du patient, du soignant, du contexte de déploiement
- Centraliser la formation et la recherche en matière d'IA, avec les financements adéquats
- Maintenir l'obligation de formation, remise en question par le Digital Omnibus, du personnel utilisant et surveillant les systèmes d'IA
- Impliquer de manière obligatoire l'APD a priori dans le traitement des données à caractère personnel médicales
- Confier un rôle explicite de protection des données médicales à l'APD

Concernant le financement :

- Structuration du développement d'IA en Belgique
- Besoin de modèles en accès ouvert que le médecin peut implémenter dans sa pratique et personnaliser pour chaque patient (biais favorables), cela implique des subsides pour la science ouverte et le développement d'écosystèmes d'IA cohérents, avec des panels différents pour différentes maladies et différents types de population
- Préserver des financements publics pérennes et structurés pour le développement de systèmes d'IA, et en particulier pour les pathologies exclues jusqu'à présent comme les maladies rares

- Utiliser la valeur des données de santé dans le cadre du développement d'outils d'IA (responsabilité sociétale des développeurs qui s'enrichissent sur le dos des consommateurs/patients) pour financer le système belge des soins de santé : changer la règle du jeu et mettre au point des règles qui créent de la valeur ajoutée pour les citoyens
- Coordination des différents niveaux de pouvoir, intégrer l'IA dans la CIM Santé Publique
- Garantir l'accessibilité des meilleurs soins pour tous et lutter contre le risque d'une médecine à deux vitesses selon que l'IA est utilisée ou pas, besoin de chartes et de contrôle

Concernant les prestataires de soin :

- Instaurer une formation IA continue obligatoire des prestataires de soins, aussi pour ceux déjà en exercice : besoin de structuration et d'harmonisation au niveau fédéral
- Adapter la déontologie en incluant la responsabilité en cas d'aide IA à la décision
- Consacrer le temps libéré par le recours à l'IA à l'accompagnement (humain) du patient

Concernant les systèmes d'IA médicaux

- Créer un organisme central de validation, d'accréditation et de contrôle pour les systèmes d'IA médicaux qui entrent sur le territoire belge (proposition : sur le modèle de ce qui fonctionne pour l'accréditation des médicaments ou l'AFSCA, créer une institution de contrôle indépendante chargée d'autoriser, de réguler et de contrôler les systèmes algorithmiques et/ou d'IA tout au long de leur durée de vie, avec accès aux données d'entraînement, au code source, aux résultats des tests, avec le pouvoir d'obliger un testing préalable à l'accréditation)
- Rendre contraignants les tests sur les biais avant toute mise en service d'un système d'IA médical
- Prise en considération de données holistiques dans les modèles (choix de vie) // droits du patient
- Participatory Design : (large) participation des médecins aux développements des systèmes d'IA médicaux
- Réfléchir en amont de l'automatisation aux types de données nécessaires et également à comment rendre chaque étape du processus de décision compréhensible et contrôlable
- Inclure, dans les requis du développement, les besoins d'information aux médecins pour
 - o 1) qu'ils puissent comprendre le fonctionnement du système d'IA,
 - o 2) qu'ils puissent l'expliquer aux patients
- Financer les hôpitaux pour les contraintes nouvelles que l'IA et la gestion des données font peser sur eux

Concernant les patients

- Campagne d'information à destination des citoyens sur l'espace européens des données et sur la possibilité de s'y opposer et comment procéder
- Remboursement d'applications médicales, sans surcoût lié à la situation de handicap
- Développer et renforcer la littératie en soins de santé des Belges
- Assurer l'accompagnement des patients moins autonomes ou éloignés des soins, créer de nouveaux métiers d'accompagnement aux soins

Concernant les hôpitaux et les centres de soins

- Qualité des soins uniforme dans tous les lieux de prise en charge
- Renforcement de cybersécurité et accompagnement, y compris financier, de la montée en cybermaturité des hôpitaux
- Garantir, dans tous les hôpitaux, la présence de l'expertise nécessaire pour analyser et critiquer les modèles d'IA
- Veiller au suivi de formation du personnel hospitalier afin de garantir la qualité de la supervision humaine en matière d'IA

- Ancrer les principes déontologiques de bienveillance (adoption de l'IA si et seulement si meilleure performance), information au patient, autonomie du patient, consentement (véritablement éclairé du patient

Concernant les développeurs de systèmes d'IA en soins de santé

- Créer un cadre national de qualité pour l'IA en s'inspirant des travaux de recherche menés dans les Hautes Ecoles Thomas More et Artevelde
(https://res.cloudinary.com/deueykgii/raw/upload/v1760560857/SWVG_Kwaliteitskader_-_aftoetsingsinstrument_p9s2yz.xlsx?_a=DATAg1RgZAA0)
- Imposer des normes de qualité méthodologiques portant sur le choix des échantillons soumis aux tests et aux évaluations afin que ces échantillons soient conformes aux exigences de la science médicale, suffisamment représentatifs et diversifiés
- Imposer d'impliquer, dans le développement des systèmes d'IA médicaux, des médecins, des associations de consommateurs et/ou de patients, des défenseurs des droits humains
- Imposer la mention des sources des décisions médicales proposées par l'IA auxquelles le médecin ET le patient doivent avoir accès
- Intégrer au maximum les droits des patients dans une application d'IA destinée aux soins de santé, par exemple en imposant un cadre dans lequel l'application concernée informe sur cette intégration : par exemple en matière d'objectifs de soins personnels, de prise de décision partagée, etc.

7/ Glossaire

AI-Act : Règlement européen relatif à l'intelligence artificielle

APD : Autorité de Protection des Données

CEDH : Convention Européenne des droits de l'homme

CIM : Conférence interministérielle

CISO: Chief Information Security Officer

CSNPH: Conseil Supérieur National des Personnes Handicapées

DPO : Data Protection Officer

EHDS: European Health Data Space

IA : Intelligence artificielle

RGPD : Règlement Général de Protection des Données