Ceraps
UMR 8026 - CNRS

Appel à communications

Université de Lille

La souveraineté sanitaire à l'ère du numérique, perspectives nationale et européenne.

Colloque organisé par le Master 2 de Droit du numérique de l'Université de Lille et l'équipe de recherche en droit du numérique du CERAPS.

Le **13 juin 2024** à la faculté des sciences juridiques, politiques et sociales de Lille.

L'évolution des technologies numériques a eu un retentissement massif sur le domaine de la santé, à l'échelle nationale comme internationale, amplifié par la pandémie de Covid-19. À travers ces mutations, la notion de souveraineté a pu être redéfinie, contestée, renforcée, ou repensée ; elle a en tout cas été questionnée et remise au premier plan du discours politique.

Afin d'en explorer les enjeux juridiques et sociétaux, le Master 2 de Droit du numérique et du cyberespace de l'Université de Lille et l'équipe de recherche en droit du numérique proposent cette année un colloque dédié au sujet de la souveraineté en matière de santé numérique. Cet évènement, ouvert à tous ceux et celles qui souhaitent partager leurs recherches liées à ce sujet, abordera un ensemble de thèmes qui reflète la complexité des enjeux actuels.

La souveraineté fait référence à une puissance ou un organe qui, concernant une compétence, n'est soumis à aucun autre. Dès lors, cette notion pourra être interrogée du point de vue du droit interne, la souveraineté étant un élément central de la Constitution et de l'histoire de l'État. Mais cette interrogation peut aussi s'orienter vers l'Union européenne, car bien que la réalité d'une souveraineté de l'Union soit discutée, il est indéniable qu'une partie des prérogatives des États lui soit déléguée, car exercée en son sein en commun par les États-membres.

Si la souveraineté sanitaire fait l'objet de nombreux débats actuellement, ce sont les aspects numériques de la santé qui retiendront ici notre attention, devant l'encadrement juridique spécifique au numérique qui connaît en ce moment une évolution inédite. En effet que ce soit à propos de la production et de l'approvisionnement en produits de santé, du pilotage des établissements et systèmes de santé, ou de la représentation des populations européennes et de leurs données dans les phases de tests ou les essais cliniques, la question d'une indépendance nationale ou européenne pose autant de questions qu'en matière de médicaments ou de dispositifs médicaux non numériques.

Cependant ces enjeux sont à ajouter à ceux propres au numérique, parfois regroupés sous le terme encore jeune et aux contours flous de « souveraineté numérique », que ce soit celui de l'approvisionnement en matériaux, des infrastructures de réseau, de la capacité à concevoir des produits et donc d'être décideurs quant aux algorithmes qui seront utilisés, de la sécurité et des frontières dans le cyberespace, d'assurer le respect du droit interne et notamment des droits fondamentaux des individus, ou encore de la capacité des États à maintenir leur souveraineté quand les éléments qui précèdent sont possédés et décidés par de puissants acteurs privés, d'autant plus non-européens.

Ainsi, des initiatives juridiques nouvelles s'appliquent au numérique dans le domaine de la santé, tout comme des textes et principes préexistants s'adaptent aux outils innovants. Citons à titre d'exemple la loi pour une République numérique et le projet de loi visant à sécuriser et réguler l'espace numérique (SREN), le règlement européen sur la gouvernance des données, celui plus récent sur l'accès équitable aux données, les directives sur la sécurité des réseaux et des systèmes d'informations (NIS I et II), le projet de règlement sur l'intelligence artificielle ou encore celui sur l'espace européen des données de santé, qui auront des incidences sur le secteur de la santé, aux différents niveaux de sa gouvernance.

Plus spécifiquement, les données sont l'objet d'enjeux forts, notamment en termes de droits fondamentaux. À l'ère numérique les frontières tendent à s'effacer, en particulier en ce qui concerne le partage et l'hébergement des données. Le respect de la vie privée, de l'intégrité des données personnelles comme celles concernant le système de santé doivent être rigoureusement préservées pour garantir les droits des patients comme des professionnels de santé. Alors que les données sont de plus en plus ouvertes à l'échelle européenne et internationale, il est essentiel de comprendre comment l'encadrement du numérique en santé influence la manière dont l'intégrité et la confidentialité des données seront assurées dans ce nouveau paradigme. Ces enjeux sont fortement liés à ceux de cybersécurité, dont le cadre juridique évolue nationalement comme supra-nationalement, avec la directive NIS précédemment évoquée et la plus récente NIS II qui devrait être transposée en droit français au cours de l'année, mais aussi le futur règlement sur la cyber-résilience ou encore celui sur la cyber-solidarité, qui concernent explicitement le secteur de la santé et ses enjeux spécifiques. Les patients utilisateurs, les professionnels de santé, les structures de soin, la continuité de ces derniers ou encore les systèmes de santé dans leur intégralité sont particulièrement vulnérables à d'éventuelles attaques ou arrêt des systèmes d'information. En matière de cybersécurité, la souveraineté, tant nationale que de l'Union européenne, est en jeu.

En effet, la place des acteurs étrangers dans le secteur du numérique – y compris en santé – est un sujet d'intérêt majeur. L'Union européenne est le théâtre d'une multitude de coopérations régionales et internationales. Elles donnent lieu à l'ouverture des données, au développement des données massives et aux espaces de partage de données : la pratique des soins de santé et la recherche privée comme publique ne se limitent plus aux seules données locales ou nationales. Les pays et infrastructures médicales ouvrent leurs bases d'informations pour permettre un marché unique et la libre circulation de produits et services de santé numérique, ce qui est à l'origine entre autres de l'Espace européen de données de santé, mais aussi de la Plateforme des données de santé en France, entraînant une métamorphose de la manière dont les soins de santé sont dispensés aux citoyens de toute l'Union, ainsi que le contrôle que ces derniers ont sur leurs données tant dans leur pays d'origine que dans les États membres de l'UE, voire au-delà.

Cette ouverture, allant de pair avec la libre circulation des données, biens et services de santé au sein de l'Union, laisse entrevoir l'importance d'une vision supranationale cohérente pour protéger de manière efficace les droits des individus, relatifs à la santé comme à la vie privée. Face à cela, la préservation du modèle national de système de santé peine à trouver sa place dans la numérisation du secteur. Pour autant, afin de respecter des exigences éthiques fortes garantissant que les progrès technologiques ne se fassent pas au détriment de l'intérêt des patients, des praticiens, et de la société dans son ensemble, cette réflexion semble devoir être menée à plusieurs niveaux, amenant des questionnements tant quant à la souveraineté nationale qu'à la place de l'UE dans un marché numérique mondial.

Ainsi, le domaine de la santé est vaste et en constante évolution. Il offre de nombreux champs de réflexion pouvant s'incarner dans les contributions de chercheurs et chercheuses, de doctorantes et doctorants, et de professionnels des secteurs privé comme public au cours de ce colloque.

Nous vous invitons à participer à cette journée d'échanges et à explorer de nouvelles idées pouvant contribuer à l'avancement des connaissances autour de ce thème. Toutes les contributions qui nous parviendront selon les modalités ci-dessous seront étudiées, des sciences juridiques comme d'autres disciplines en lien avec le sujet.

Modalités de candidature

Les propositions de contribution sont à envoyer jusqu'au 29 mars 2024 à l'adresse suivante :

colloque-cyberdroit@univ-lille.fr

Cette proposition de contribution consiste en un résumé du propos qui serait présenté, limité à 2 pages (ou environ 1000 mots hors notes de bas de page et bibliographie). **Une réponse sera donnée aux candidats le 10 avril au plus tard**.

Les propositions de contribution ne doivent pas comporter de références personnelles dans le texte ou sur le document, les noms et affiliations des auteurs et autrices devront être mentionnés dans l'e-mail qui l'accompagne, afin de respecter le processus de sélection anonymisé.

Les frais de transport et d'hébergement sur le lieu du l'évènement pourront être pris en charge pour les personnes sélectionnées, sur demande au comité d'organisation.

Pour toute question, merci de contacter **audrey.dequesnes@univ-lille.fr** ou **colloque-cyberdroit@univ-lille.fr**