CYBERSÉCURITÉ EN MATIÈRE DE DONNÉES DE SANTÉ : UN ENJEU STRATÉGIQUE POUR NOTRE SOCIÉTÉ

Anne LE HENANFF

- Députée Horizons et App. du Morbihan
- Membre de la commission de la Défense nationale et des Forces armées
- Vice-présidente du groupe d'études Économie, sécurité et souveraineté numériques
- Membre de la Commission mixte paritaire du projet de loi visant à sécuriser et réguler l'espace numérique (SREN)

Comme le rappelait dernièrement la présidente de l'Agence du numérique en santé, « le numérique en santé n'est plus une option, il est déjà une réalité aujourd'hui et le sera encore plus demain ».

La transformation numérique dans le domaine de la santé, de l'usage de l'intelligence artificielle à la dématérialisation, ne fait plus aucun doute et ne cesse d'ouvrir de nouvelles possibilités, c'est pourquoi elle est étroitement accompagnée par le gouvernement, via la direction du Numérique en santé (DNS) et l'Agence du Numérique en santé (ANS). Mais au-delà de l'enjeu technologique, se pose la question de la confiance en ces nouveaux outils numériques.

Si 90 % des Français ont déjà eu recours à au moins un service numérique de santé, ils sont presque aussi nombreux à considérer leurs données de santé comme particulièrement sensibles et redoutent qu'elles soient utilisées à des fins commerciales ou soient cyber attaquées.

Dans un contexte de cyberattaques croissantes envers les établissements de santé et les sites hébergeant des données de santé, il est nécessaire que les législateurs se saisissent de la cybersécurité et de la souveraineté de l'hébergement des données de santé.

En ce sens, le programme CaRE (cybersécurité, accélération et résilience des établissements) est un objectif prioritaire de la feuille de route du numérique en santé 2023-2027.

Par ailleurs, au-delà des divers accompagnements et dispositifs, mis en place par l'ANS et l'Agence nationale de la Sécurité des systèmes d'information (ANSSI), afin de permettre une montée en compétence des établissements de santé dans le domaine cyber, des dispositions législatives et réglementaires ont été nécessaires afin de garantir la sécurité de l'hébergement de nos données.

Ainsi, la version 2024 du référentiel d'hébergement des données de santé, qui comporte désormais des exigences en matière de localisation des données au sein de l'Espace économique européen et renforce les obligations de transparence des hébergeurs quant à une éventuelle sujétion à des réglementations extra-communautaires, va dans le bon sens. Mais il nous faudra certainement aller plus loin, en y ajoutant des critères de protection contre les législations extra-européennes.

La loi « Sécuriser et réguler l'espace numérique » récemment votée au Parlement marque un tournant majeur dans l'hébergement souverain de nos données les plus sensibles.

Ce sujet a été au cœur des débats sur le Titre III relatif au Cloud dont j'étais rapporteure, avec ce même souci de renforcer l'information et la protection envers les risques d'accès aux données par des États tiers.

Ainsi, nous avons inscrit dans la loi le périmètre de la circulaire dite « Cloud au centre » assurant une transformation numérique sur le Cloud dans le strict respect de la cybersécurité et de la protection des données des opérateurs de l'État mais aussi de certaines entités dont l'activité est stratégique, tel que le Health Data Hub (HDH).

Créé pour faciliter le partage des données de santé afin de favoriser la recherche, le HDH catalyse depuis plus de quatre ans, les débats liés à la souveraineté des données en raison de l'hébergement de sa plateforme technique chez Microsoft.

Le Parlement s'est donc saisi une bonne fois pour toutes de cet enjeu majeur qui démontre que l'absence de confiance peut retarder la mise en place d'une solution pourtant nécessaire afin d'améliorer le fonctionnement de notre système de santé.

« Dans un contexte de cyberattaques croissantes envers les établissements de santé (…), il est nécessaire que les législateurs se saisissent de la cybersécurité »

Les débats l'ont montré, les enjeux de cybersécurité et de protection des données ne relèvent plus d'un débat d'experts et sont éminemment stratégiques pour notre société. Ainsi, le futur projet de loi « Résilience », qui viendra mettre en application des textes européens comme la directive Network and Information Security (NIS 2, renforcement de la cybersécurité), est fondamental car il clarifiera les règles que devront appliquer les organisations les plus stratégiques de notre pays. ●