ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 38995	De **M. François-Michel Lambert** (Libertés et Territoires - Bouches-du-Rhône)	**Question écrite**
Ministère interrogé > Transition numérique et communications électroniques	**Ministère attributaire** > Premier ministre	
Rubrique >numérique	**Tête d'analyse** >Sécurité des automates connectés médicaux	**Analyse** > Sécurité des automates connectés médicaux.
Question publiée au JO le : **18/05/2021** Réponse publiée au JO le : **10/05/2022** page : **3134** Date de changement d'attribution : **08/06/2021**		

Texte de la question

M. François-Michel Lambert attire l'attention de M. le secrétaire d'État auprès des ministres de l'économie, des finances et de la relance, et de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques, sur la sécurité informatique des automates connectés dans le domaine médical. Ces automates connectés regroupent un ensemble de matériels médicaux : nutripompes, respirateurs, dialyseurs, etc. Si la sécurité de l'information et des systèmes informatiques des hôpitaux est un sujet crucial et a déjà été soulevée dans de précédentes questions, la sécurité des automates connectés est elle aussi indispensable pour garantir la sécurité des soins aux Français. Or elle n'est pas garantie comme l'ont démontré les multiples cyberattaques contre les hôpitaux et le rapport « *Common Situational Picture* » de l'ANSSI et du BSI. Les spécialistes font le constat qu'une majorité d'automates connectés ne sont pas ou mal protégés, qu'ils portent des systèmes obsolètes datant d'il y a entre 5 et 10 ans et qu'ils sont vulnérables aux attaques malveillantes (arrêts systèmes, *ransomwares*, etc.). La réglementation actuelle est elle aussi obsolète et date des années 2000, les fournisseurs refusent que leurs matériels soient testés et l'ANSSI ne traite pas spécifiquement la sécurité des automates connectés alors que cela pourrait tout à fait être décidé. Dans le contexte de la crise sanitaire, l'insécurité sur des objets médicaux indispensables appelle une réponse urgente et forte pour éviter des futures paralysies du système hospitalier, des piratages de données sensibles et des sabotages de matériels médicaux. Par conséquent, il lui demande de préciser les moyens que compte mettre en œuvre le Gouvernement pour pallier ces risques et dans quel délai.

Texte de la réponse

La mise en réseau, au moyen d'Internet, d'objets physiques autres que les terminaux informatiques (montre, thermostat, caméra, etc.) soulève de forts enjeux de sécurité numérique. En effet, la multiplication de ces objets connectés vient accroître la « surface d'attaque ». De plus, les industriels qui produisent ces objets connectés sont souvent moins compétents en matière de bonnes pratiques de sécurité numérique que les fabricants de terminaux numériques traditionnels. Au-delà de ces constats valables pour l'ensemble des objets connectés, les dispositifs médicaux se distinguent par l'acuité des risques causés par leur connexion à l'Internet, puisque qu'une compromission est susceptible de mettre en danger une vie humaine. Pour renforcer la sécurité des objets connectés, dont les dispositifs médicaux, le Gouvernement a initié et soutenu plusieurs initiatives visant à renforcer les responsabilités pesant sur leurs fabricants. Ces derniers étant largement localisés hors du territoire national, la

régulation des objets connectés est portée au niveaux européen et international. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a ainsi fortement contribué aux travaux de l'Organisation de coopération et de développement économique (OCDE) sur la sécurité de l'économie numérique qui ont fait émerger des responsabilités devant reposer sur les fabricants d'objets connectés (mise en place d'un processus de divulgation responsable des vulnérabilités, garantie d'une durée minimale de disponibilité des correctifs de sécurité, etc.). Le projet de règlement européen sur la cyber-résilience pourra de fait constituer un véhicule législatif approprié pour retranscrire les conclusions de l'OCDE et s'assurer que les objets connectés vendus en Europe respectent les plus hauts standards de sécurité. En sus de ces normes de cybersécurité qui concernent l'ensemble des objets connectés, des obligations spécifiques pèsent sur les dispositifs médicaux. Le règlement (UE) 2017/745 en date du 5 avril 2017 relatif aux dispositifs médicaux a ainsi renforcé les obligations pesant sur les fabricants de dispositifs médicaux en prévoyant notamment une évaluation renforcée de leurs solutions. Il est important de noter que la sécurité des dispositifs médicaux dépend également de leur environnement, et notamment des réseaux auxquels ils se retrouvent connectés. La sécurité de ces dispositifs ne peut donc être envisagée en isolation de la question de la sécurité numérique des systèmes de santé. Le Gouvernement a engagé depuis 2019 une action résolue en vue d'accroitre la maturité des établissements de santé en matière de cybersécurité. Le plan France Relance a permis à plus d'une centaine d'entre eux de bénéficier d'un parcours de cybersécurité sous l'égide de l'ANSSI, comprenant un diagnostic de cybersécurité puis un accompagnement immédiat en vue d'accroitre le niveau de sécurité.