ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 15289	De **M. Sébastien Peytavie** (Écologiste - NUPES - Dordogne)	**Question écrite**

Ministère interrogé > Santé et prévention	**Ministère attributaire** > Santé et prévention

Rubrique >assurance complémentaire	**Tête d'analyse** >Réaction face à la cyberattaque à l'encontre de gestionnaires de tiers payant	**Analyse** > Réaction face à la cyberattaque à l'encontre de gestionnaires de tiers payant.

Question publiée au JO le : **20/02/2024**
Question retirée le : **11/06/2024** (fin de mandat)

Texte de la question

M. Sébastien Peytavie alerte M. le ministre délégué auprès de la ministre du travail, de la santé et des solidarités, chargé de la santé et de la prévention sur le récent piratage massif des données informatiques de santé ; le secteur de la santé étant aujourd'hui de plus en plus exposé aux risques de cybercriminalité. Alors que 33 millions de Françaises et de Français sont concernées et concernés par ce vol de données de santé, la question de la protection, de l'information et de la prévention des citoyens et des citoyennes se pose. En effet, la France pays a subi une cyberattaque inédite extorquant à un ou une Français ou Française sur deux des informations telles que l'état civil, le numéro de sécurité sociale, la date de naissance, le nom de l'assureur santé ainsi que les garanties du contrat souscrit. Ces attaques concernent les deux principaux acteurs du tiers-payant chargés des complémentaires santé et des mutuelles : Viamedis et Almerys. Suite à cette attaque, la Commission nationale de l'informatique et des libertés a appelé les Françaises et les Français à surveiller les activités de leurs comptes bancaires. Depuis l'an passé, la cybercriminalité ne cesse de s'étendre et gagne de plus en plus le champ de la santé, avec des risques réels pour la protection des données personnelles des patients et des patientes, en particulier les plus vulnérables. Ces attaques se multiplient et les systèmes informatiques sont manifestement insuffisamment préparés pour y faire face. Bien que les données de contact ne soient pas concernées par la violation, il est facile pour les pirates d'adjoindre les informations récoltées à d'autres données volées pour persuader les personnes ciblées de renseigner leur numéro de carte bancaire. Au-delà des risques imminents d'escroquerie, cette cyberattaque pourrait également comporter un risque relatif au remboursement des soins de santé. Certains professionnels et certaines professionnelles de santé pourraient, en effet, être amenés et amenées à refuser l'avance des frais aux adhérents et adhérentes des deux sociétés piratées puisque les plateformes de remboursement s'avèrent dans l'immédiat indisponibles. Il l'interroge ainsi sur les mesures envisagées afin d'informer les personnes visées par cette attaque sur les risques d'escroquerie à venir et de renforcer la sécurité des données de santé pour prévenir durablement de nouvelles attaques.