

## 15ème législature

<b>Question N° :</b> <b>21315</b>	De <b>M. Thibault Bazin</b> ( Les Républicains - Meurthe-et-Moselle )	<b>Question écrite</b>
<b>Ministère interrogé</b> > Numérique		<b>Ministère attributaire</b> > Premier ministre
<b>Rubrique</b> >numérique	<b>Tête d'analyse</b> >Objets connectés - Risques	<b>Analyse</b> > Objets connectés - Risques.
Question publiée au JO le : <b>09/07/2019</b> Réponse publiée au JO le : <b>09/03/2021</b> page : <b>2015</b> Date de changement d'attribution : <b>15/12/2020</b> Date de renouvellement : <b>03/12/2019</b> Date de renouvellement : <b>16/06/2020</b> Date de renouvellement : <b>01/12/2020</b>		

### Texte de la question

M. Thibault Bazin attire l'attention de M. le secrétaire d'État auprès du ministre de l'économie et des finances et du ministre de l'action et des comptes publics, chargé du numérique, sur les menaces, en termes de sécurité, que représentent les objets connectés. Ce marché est en plein essor puisque les chiffres rendus publics par le cabinet GfK en 2018 ont annoncé une croissance de 33% en un an. Ces objets connectés touchent beaucoup de domaines comme la maison, avec les appareils dédiés à la sécurité et à l'automatisation, les appareils d'électroménager, mais aussi les domaines du sport et de la santé avec notamment le développement des montres et bracelets connectés. Beaucoup d'informations transitent donc sur ces appareils. Deux risques se développent : celui de l'utilisation commerciale des données personnelles et les atteintes à la vie privée et le risque du piratage. Il vient lui demander ce que le Gouvernement compte faire pour mieux protéger les utilisateurs de ces risques et mieux les informer sur ceux-ci.

### Texte de la réponse

La notion d'objet connecté recouvre une grande variété de dispositifs pour lesquels les exigences de sécurité ne peuvent être identiques. Ainsi, un dispositif médical de régulation et de stimulation cardiaques connecté devra nécessairement répondre à des exigences de sécurité très élevées. A contrario, la sécurisation d'un objet connecté dont l'usage ne présente pas de risque pour l'utilisateur, comme une commande à distance de luminaire ou de dispositif musical par exemple, pourra se limiter à des exigences telles qu'un mot de passe conforme à des recommandations simples, une protection des flux de données standardisées ou un système d'exploitation dûment mis à jour. Le cadre de certification européen, établi par le Cybersecurity Act adopté le 7 juin 2019, prend en compte cette diversité d'objets connectés en proposant des niveaux de certification distincts, allant de « faible » à « élevé ». L'Agence nationale de la sécurité des systèmes d'information (ANSSI) sera chargée de l'application de ce cadre de certification en France. Par ailleurs, des travaux normatifs sont également en cours dans les enceintes techniques européennes et internationales pour poser des principes de cybersécurité applicables à tous les objets connectés, tout au long de leur durée d'utilisation.