ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 3751	De **M. Luc Carvounas** (Nouvelle Gauche - Val-de-Marne)	**Question écrite**

Ministère interrogé > Numérique	**Ministère attributaire** > Numérique

Rubrique >Internet	**Tête d'analyse** >Risques d'atteinte à la vie privée par les objets connectés	**Analyse** > Risques d'atteinte à la vie privée par les objets connectés.

Question publiée au JO le : **12/12/2017**
Réponse publiée au JO le : **20/03/2018** page : **2348**

Texte de la question

M. Luc Carvounas attire l'attention de M. le secrétaire d'État, auprès du Premier ministre, chargé du numérique, sur les risques d'atteinte à la vie privée par les objets connectés. À l'approche des fêtes de fin d'année la CNIL a alerté les consommateurs sur les risques d'atteinte à la vie privée des propriétaires d'objets connectés. Des jouets connectés comme une poupée « intelligente » qui répond aux questions des enfants *via* une application ou les enceintes munies d'assistants vocaux provoquent l'inquiétude des défenseurs des libertés numériques. Ces objets connectés munis d'enregistreurs et de micros ont donc la capacité d'écouter les conversations et de transmettre des informations. Les fabricants ont donc l'opportunité de collecter des données privées à visées publicitaires. Aux États-Unis, une grande enseigne de fast-food a même réussi à pirater des assistants vocaux *via* une diffusion télévisuelle afin d'y imposer leur publicité. Ces objets connectés, souvent fabriqués à l'étranger, peuvent donc cibler les potentiels clients dans un but publicitaire mais surtout espionner les conversations privés aux dépens des usagers et de leurs entourages. Il lui demande donc quelles mesures compte prendre le Gouvernement afin de protéger les propriétaires d'objets connectés.

Texte de la réponse

Le renforcement de la protection des données personnelles de nos concitoyens est l'objectif premier du règlement européen sur la protection des données (RGPD), qui entrera en application le 25 mai 2018. Celui-ci fixe un cadre global renforcé, et unifié au niveau européen, pour la protection des données personnelles à toutes les étapes de leur traitement et par l'ensemble des acteurs concernés par ces traitements. Il s'appliquera donc notamment aux fournisseurs d'objets connectés, et en particulier aux plateformes associées qui centralisent et traitent les données de ces objets. Par ailleurs et de manière complémentaire, l'État Français contribue activement à l'élaboration en cours, sous l'impulsion de la Commission Européenne, d'un cadre européen unifié de certification de la sécurité des produits et services numériques. Ce cadre, que la France appelle de ses vœux depuis plusieurs années, et qui fédérera les différents cadres réglementaires préexistants au niveau national, permettra d'offrir aux différents acteurs (consommateurs, administrations, entreprises) des garanties fiables sur les propriétés de sécurité des solutions numériques, notamment en matière de protection des données. Il pourra au besoin servir de base normative à l'élaboration de règlementations complémentaires, pour couvrir des enjeux spécifiques, par exemple sectoriels. L'ANSSI, chef de file national dans le cadre des négociations en cours sur ce cadre, et disposant par ailleurs d'une expertise largement reconnue en Europe sur ces thématiques, promeut à cette fin une vision exigeante quant aux garanties de sécurité apportées par la certification, tout en veillant à préserver la souplesse et l'adaptabilité des méthodes de certification afin de leur permettre de couvrir les usages émergents, dont les objets

connectés.