

15ème législature

Question N° : 40563	De M. Pierre Venteau (La République en Marche - Haute-Vienne)	Question écrite
Ministère interrogé > Transition numérique et communications électroniques		Ministère attributaire > Premier ministre
Rubrique > Internet	Tête d'analyse > Enjeux locaux liés à la cyber-sécurité	Analyse > Enjeux locaux liés à la cyber-sécurité.
Question publiée au JO le : 03/08/2021 Réponse publiée au JO le : 03/05/2022 page : 2943 Date de changement d'attribution : 24/08/2021		

Texte de la question

M. Pierre Venteau 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 les compétences des collectivités territoriales en matière de cyber-sécurité. L'affaire Pegasus, portée à l'attention du public le 19 juillet 2021, a souligné la nécessité de se doter d'outils de cyberdéfense efficaces. Les collectivités locales sont des cibles particulièrement vulnérables. Pourtant beaucoup estiment aujourd'hui que la cyber sécurité n'entre pas dans leurs prérogatives et manquent d'outils pour garantir leur sécurité informatique. Avec le développement des *smart cities*, la capacité des administrations locales à assurer leur protection devient un enjeu majeur. M. le député demande donc si l'attribution d'une compétence de cyber-sécurité est envisageable à l'échelle locale, notamment par la mise en place d'un référent cyber-sécurité au sein des EPCI, accompagnée d'une possibilité de former les élus locaux aux risques cyber. Dans ce cadre, le projet de loi 3DS en cours de discussion pourrait constituer un vecteur législatif particulièrement adapté. Il souhaite connaître son avis sur le sujet.

Texte de la réponse

Les collectivités locales sont fréquemment la cible de cyberattaques, principalement criminelles, visant à les rançonner en paralysant leurs systèmes d'information et en les empêchant ainsi de remplir leurs missions. La vie de la population en est directement affectée, dans la mesure où les collectivités locales gèrent des transports publics, des prestations sociales ou encore l'état-civil. La numérisation croissante des acteurs administratifs, souvent peu conscients de leur vulnérabilité aux cyberattaques, en fait des victimes de choix pour les attaquants. L'émergence de smart cities laisse craindre une future aggravation de ces phénomènes. Sans préjudice de l'attribution d'une compétence en matière de cybersécurité, il est important de souligner que les collectivités territoriales sont d'ores et déjà soumises à un certain nombre d'obligations en matière de cybersécurité, tant pour protéger les données personnelles de leurs usagers au titre du règlement général sur la protection des données personnelles que pour sécuriser leurs échanges avec le public. Tout directeur d'établissement exploitant des outils numériques pour le fonctionnement de son établissement se doit ainsi d'en assurer la sécurité et peut pour cela s'appuyer sur de nombreuses ressources. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a ainsi publié plusieurs guides à destination des collectivités territoriales, pour leur venir en aide dans leur démarche de renforcement de leur cybersécurité. De surcroît, l'ANSSI arme un dispositif de délégués régionaux en mesure de



conseiller les collectivités territoriales dans le choix d'outils de cybersécurité. Elle a également noué des partenariats avec des associations représentant les fournisseurs de services des collectivités territoriales pour renforcer en amont la cybersécurité de ces services. Dans le cadre du plan de relance, un parcours de cybersécurité a également été développé. Il ouvre droit à financement pour les collectivités volontaires qui souhaitent évaluer leur niveau de cybersécurité, identifier des mesures de sécurisation à prendre en urgence et établir une feuille de route de renforcement de leur cybersécurité. De surcroît, le plan de relance finance un appel à projets d'installation à grande échelle d'outils de cybersécurité, en coopération avec des fournisseurs de services numériques aux collectivités territoriales. Ces dispositifs nécessiteront être pérennisés. En l'état actuel des choses, le recours à la loi ne constitue pas un prérequis mais pourrait contribuer à cette pérennisation.