ASSEMBLÉE NATIONALE

17ème législature

Sécurité des données numériques

Question écrite n° 485

Texte de la question

Mme Géraldine Bannier attire l'attention de Mme la secrétaire d'État auprès du ministre de l'enseignement supérieur et de la recherche, chargée de l'intelligence artificielle et du numérique, sur le sujet de l'accessibilité et de la sauvegarde des données numériques des citoyens français. De fait, depuis quelques années maintenant, la France s'est engagée dans un mouvement de numérisation de ses documents administratifs : fiches de paie, trimestres cotisés, données financières ou relatives à la santé. Les exemples sont nombreux et concernent des domaines de première importance. Les documents des ressources humaines sont un exemple parlant : depuis le 1er janvier 2017, la loi du 8 août 2016 « relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels » facilite la dématérialisation des fiches de paie et autres documents des ressources humaines au sein des entreprises. Afin de sécuriser l'accès des employés aux documents, l'employeur est dans l'obligation de pouvoir les leur fournir pour une durée de 50 ans, ou jusqu'à l'âge de la retraite, augmenté de 6 ans. Il doit également garantir la confidentialité de ces données. Cela s'effectue *via* le compte personnel d'activité, grâce auquel chaque employé peut consulter les documents dématérialisés dans un coffre-fort numérique. Si cette dématérialisation présente de nombreux avantages, comme un gain de temps ou encore un accès facilité - l'intelligence artificielle étant associée à une productivité accrue - la numérisation des données des Français soulève des questions d'accessibilité pérenne à ces documents. En effet, ces datas peuvent, entre autres, être soumises à un risque de cyberattaque. En 2021, 582 établissements hospitaliers français ont été victimes d'une attaque de ce type, soit un établissement sur six. Selon le baromètre du CESIN (Club des experts de la sécurité de l'information et du numérique), une entreprise française sur deux a été victime d'une agression numérique en 2022. Ces chiffres posent la question de la fiabilité de la conservation des données. La sécurité des équipements permettant l'hébergement des données est également en cause, à un second niveau. Le numérique n'est pas seulement un objet éthéré et immatériel : il repose sur des installations informatiques bien tangibles et qui peuvent être sujettes à des incendies, des dégradations, des pannes d'électricité. Les câbles sous-marins peuvent subir des attaques. La question se pose donc au niveau national et international : comment garantir la sauvegarde à longue échéance des données de santé, des données ouvrant des droits sociaux comme le nombre de trimestres cotisés, par exemple ? Sans doute la réponse repose-t-elle sur des moyens matériels et humains suffisants pour produire la forme de résilience nécessaire. La formation, tant des citoyens - parfois en incapacité d'accéder à leurs données - que des professionnels, qui doivent pouvoir s'adapter aux évolutions permanentes, est primordiale. À l'ère du soupçon et des fausses vérités, c'est ainsi, au final, la confiance des concitoyens qui est au cœur des enjeux. Elle souhaite connaître son avis sur le sujet.

Texte de la réponse

Bien qu'il soit un important levier de transformation, le déploiement des technologies numériques s'accompagne également de nouveaux risques qu'il convient de maîtriser. Ces risques peuvent avoir une origine malveillante, comme dans le cas d'une cyberattaque, ou accidentelle, comme dans le cas d'une catastrophe naturelle qui endommagerait les infrastructures physiques sur lesquelles reposent les systèmes d'information. Dans tous les cas, les conséquences de tels évènements peuvent s'avérer catastrophiques en raison de l'omniprésence des

technologies de l'information et de la communication dans l'ensemble des organisations. Dans le secteur des activités sociales et de santé, le besoin de conservation sur une longue durée des données nécessaires à la gestion des retraites, ou encore le besoin de disponibilité des applications utilisées dans la prise en charge des patients, illustrent bien l'enjeu de maîtrise des risques relatifs au numérique. Dans ce contexte, différents dispositifs existent pour répondre à cet enjeu. Sur le plan réglementaire, la politique de sécurité des activités d'importance vitale a intégré dès 2013 des obligations en matière de sécurité des systèmes d'information applicables aux opérateurs publics et privés identifiés comme indispensables pour la continuité d'activité de la Nation. Cette approche a été étendue à l'échelle européenne en 2016, avec la publication d'une première directive dite NIS, relative à la sécurité des réseaux et des systèmes d'information dans l'Union. Transposée en droit national en 2018, ce texte concerne environ 300 opérateurs fournissant des services essentiels, dont près de la moitié dans le secteur de la santé et de la protection sociale. La même année est entré en vigueur le règlement général sur la protection des données traitant plus spécifiquement de la protection des données à caractère personnel, dont les données des assurés sociaux et les données de santé. Plus récemment, la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique a introduit de nouvelles dispositions concernant le recours aux services d'informatique en nuage pour la conservation des données stratégiques et sensibles des administrations de l'État, de ses opérateurs et de certains groupements d'intérêt public, comme la plateforme des données de santé, face aux risques que font peser les législations non-européennes sur ces données. Différentes actions ont été mises en place, notamment par l'Agence nationale de la sécurité des systèmes d'information, afin d'accompagner les entités concernées par ces réglementations – et de façon générale toute organisation concernée par ces enjeux – dans la sécurisation de leurs systèmes d'information et leur maturation cybersécuritaire. Maîtrisant parfaitement la typologie des menaces pesant sur les systèmes d'information et des moyens permettant de s'en prémunir, l'ANSSI met à la disposition de la population de nombreuses ressources de sécurisation, tant organisationnelles que techniques. Vis-à-vis des enjeux de conservation des données ou de continuité d'activité face à une cyberattaque, l'ANSSI publie par exemple un document de recommandations consacré à la sauvegarde des systèmes d'information, dans lequel figure la règle dite « 3 – 2 – 1 » : 3 copies de la sauvegarde sur 2 supports différents dont 1 hors ligne. L'ANSSI est également amenée à apporter un accompagnement personnalisé aux acteurs de l'administration et aux entités les plus "critiques" dans la sécurisation de leurs systèmes d'information. L'ANSSI a par ailleurs piloté le volet cybersécuritaire du plan France Relance. Ce programme a notamment permis d'apporter un soutien méthodologique et financier à plus de 900 entités publiques parmi les plus vulnérables (collectivités locales, établissements publics ciblés, établissements de santé) via des parcours de cybersécurité comprenant une phase de diagnostic et une phase de mise en œuvre des actions, pour un montant total de 100 millions d'euros. Capitalisant sur ces travaux, l'action du Gouvernement s'intensifie pour faire face à une menace devenue systémique, dans un contexte géopolitique qui ne fait que se dégrader. Le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité en cours d'examen au Parlement vise à transposer notamment une version révisée de la directive NIS. A l'issue, près de 15 000 organisations, dont de nombreuses entités de l'administration publique et du secteur de la santé, seront incluses dans le champ des acteurs soumis à des obligations légales en matière de sécurité des systèmes d'information (incluant des mesures de protection physique des infrastructures sous-jacentes). Dans ce contexte, l'ANSSI adapte son offre d'accompagnement au volume et à la nature des acteurs concernés. Le lancement récent de la plateforme « MesServicesCyber », visant à rendre accessibles au plus grand nombre les ressources et services de l'ANSSI, participe notamment au changement d'échelle devenu indispensable pour répondre efficacement aux risques liés au numérique. L'ANSSI s'est également vu confier de nouvelles missions de contrôle et de supervision de la mise en œuvre de la nouvelle législation. Enfin l'action de l'ANSSI en tant qu'autorité nationale de cybersécurité a également vocation à s'appuyer sur des relais indispensables, publics et privés, au sein des secteurs d'activité et des territoires. Dans le secteur de la santé, le ministère de la santé a ainsi fourni à un appui important à la cybersécurité des établissements de santé via le plan « CaRE ». Lancé en 2024, un premier volet de ce plan ciblant les principales vulnérabilités des systèmes d'information hospitaliers, doté d'une enveloppe de 65 millions d'euros, a déjà permis de réaliser des progrès importants. Un second volet, consacré à la résilience des établissements de santé, doit être lancé en 2025. Ce type d'initiative illustre l'enjeu d'une réponse collective et coordonnée face à une cybermenace en perpétuelle évolution.

Données clés

Version web : https://www.assemblee-nationale.fr/dyn/17/questions/QANR5L17QE485

Auteur : Mme Géraldine Bannier
Circonscription : Mayenne (2e circonscription) - Les Démocrates
Type de question : Question écrite
Numéro de la question : 485
Rubrique : Numérique
Ministère interrogé : Intelligence artificielle et numérique
Ministère attributaire : Premier ministre

Date(s) clée(s)

Question publiée au JO le : 8 octobre 2024, page 5166
Réponse publiée au JO le : 22 avril 2025, page 2895