ASSEMBLÉE NATIONALE

17ème législature

Stratégie de l'État en matière de cybersécurité des administrations publiques

Question écrite n° 12533

Texte de la question

M. Théo Bernhardt alerte Mme la ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique, sur la stratégie de l'État en matière de cybersécurité des administrations publiques, suite à la multiplication préoccupante des cyberattaques visant les services de l'État. La cyberattaque dont a été victime le ministère des sports en décembre 2025, ayant entraîné l'exfiltration des données personnelles de 3,5 millions de foyers français, illustre les vulnérabilités structurelles des systèmes d'information publics. Cette attaque fait suite à celle du ministère de l'intérieur quelques jours auparavant, ainsi qu'aux piratages de France Travail, de la Caisse nationale d'assurance vieillesse et de plusieurs fédérations sportives au cours des derniers mois. Ces incidents révèlent que les administrations publiques, qui imposent pourtant aux entreprises privées des obligations strictes en matière de cybersécurité et de conformité au RGPD, ne parviennent pas elles-mêmes à garantir un niveau de protection suffisant des données qui leur sont confiées par les citoyens. Les conséquences sont graves : risques accrus d'usurpation d'identité, de *phishing* ciblé et érosion de la confiance des Français envers les services publics numériques. Cette situation pose la question de l'adéquation entre les moyens alloués à la cybersécurité publique et l'ampleur des menaces, mais également celle de l'harmonisation des pratiques de sécurité entre les différentes administrations, de la vétusté de certaines infrastructures informatiques et de la capacité de l'État à conduire des audits de sécurité réguliers et efficaces. M. le député souhaite donc connaître la stratégie globale du Gouvernement pour renforcer la cybersécurité de l'ensemble des administrations publiques, ministères et établissements publics. Il l'interroge également sur les moyens budgétaires et humains spécifiquement dédiés à la protection des systèmes d'information de l'État et sur l'évolution de ces moyens au cours des trois dernières années. Il lui demande par ailleurs quels mécanismes d'audit, de contrôle et de certification de la sécurité des systèmes d'information sont mis en œuvre de manière systématique et régulière au sein des différentes administrations. Il souhaite enfin savoir comment le Gouvernement compte harmoniser les standards de sécurité entre les différents ministères et établissements publics pour éviter que les maillons faibles ne compromettent l'ensemble du système et quelles sanctions administratives sont prévues en cas de manquement caractérisé aux obligations de sécurisation des données personnelles par les responsables de traitement au sein de l'administration publique.

Texte de la réponse

La menace cyber demeure à un niveau élevé comme le démontrent d'année en année les rapports sur la cybermenace publiés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Les attaques informatiques tendent à se complexifier et affectent désormais l'ensemble de notre tissu économique et social. C'est dans cette perspective et pour préparer une menace qui devrait se durcir dans le contexte international, que le Gouvernement a présenté le 29 janvier 2026 une nouvelle stratégie nationale de cybersécurité. Cette stratégie met au cœur de ses priorités la consolidation de la sécurité des systèmes d'information de l'État. Elle s'inscrit dans la lignée des efforts continus mis en œuvre par l'État depuis plusieurs années et qui place la France au rang des pays les plus matures en matière de cybersécurité. Ces efforts se sont traduits par la structuration de la gouvernance de la politique publique de cybersécurité au sein de l'État avec la création et le développement de l'ANSSI. Ils se sont aussi traduits par d'importants investissements financiers et humains,

parmi lesquels la création de centres de réponses à incidents cyber au sein des ministères et le développement et le renforcement d'infrastructures de sécurité interministérielles. Ces efforts se sont également traduits par la création d'un cadre réglementaire qui a inspiré d'autres États et l'Union européenne. Les administrations publiques sont d'ores et déjà régulées et peuvent faire l'objet de contrôles en matière de cybersécurité à plusieurs titres, notamment : les opérateurs d'importance vitale personnes publiques en application du code de la défense, les opérateurs de services essentiels personnes publiques en application de la loi de transposition de la directive NIS 1 (Network and Information Security, sur la sécurité des réseaux et des systèmes d'information en français), en application de la politique de sécurité des systèmes d'information de l'Etat, en application de l'instruction générale interministérielle 1337. L'obligation d'assurer la sécurité des données à caractère personnel est par ailleurs prévue par le règlement général sur la protection des données (RGPD), sous le contrôle de la Commission nationale de l'informatique et des libertés (CNIL). Le législateur français a fait le choix d'exclure des amendes les situations où le traitement est mis en œuvre par l'État, « puisque la CNIL ne [dispose] pas de la personnalité morale, l'autoriser à sanctionner l'État reviendrait à considérer que celui-ci peut se verser de l'argent à lui-même » (rapport de la Commission des lois de l'Assemblée nationale / N° 1537 - Rapport de M. Francis Delattre sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (762)). Elle tend cependant à rendre publiques les mises en demeure ou les rappels à l'ordre qu'elle prononce à l'égard des ministères. Concernant les établissements publics à caractère administratif, le traitement est différemment. Dans le cadre de la décision de sanction prise à l'encontre de France Travail, la CNIL a considéré que l'établissement est « une institution nationale publique dotée de la personnalité morale et donc une entité bien distincte de l'État » et que « le traitement concerné n'est ainsi pas mis en œuvre par l'État mais par France Travail “pour le compte de l'État” […] » et a décidé qu'il était dès lors possible de prononcer une amende (décision du 22 janvier 2026). Ce cadre réglementaire sera renforcé par le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité actuellement en discussion au Parlement et qui transposera dans le droit national la directive NIS 2. Il imposera aux administrations comme à plusieurs milliers d'entreprises un socle d'exigences de cybersécurité. Il permettra ainsi d'instaurer des mesures de cybersécurité renforcées et harmonisées pour ces organisations.

Données clés

Auteur : M. Théo Bernhardt
Circonscription : Bas-Rhin (8e circonscription) - Rassemblement National
Type de question : Question écrite
Numéro de la question : 12533
Rubrique : Administration
Ministère interrogé : Intelligence artificielle et numérique
Ministère attributaire : Intelligence artificielle et numérique

Date(s) clée(s)

Question publiée au JO le : 3 février 2026, page 764
Réponse publiée au JO le : 3 mars 2026, page 1910