ASSEMBLÉE NATIONALE

17ème législature

Multiplication des fuites de données et indemnisation des victimes

Question écrite n° 14767

Texte de la question

M. Thomas Ménagé 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 progression alarmante des violations de données personnelles affectant les citoyens français, tant dans la sphère publique que privée. Entre septembre 2024 et septembre 2025, 8 613 violations de données ont été notifiées à la Commission nationale de l'informatique et des libertés (CNIL), soit une hausse de 45 % en un an, ce qui équivaut à 24 fuites par jour ou 1 fuite par heure. Le nombre de personnes affectées est désormais estimé à 12,2 millions en 2025, contre 8 millions l'année précédente et les incidents d'origine intentionnelle progressent de plus de 60 %, portés par la généralisation du *phishing*, le vol d'identifiants et les attaques externes. Les exemples récents illustrent l'ampleur systémique du phénomène : France Travail (43 millions de personnes concernées), le fichier FICOBA (1,2 million de comptes bancaires exposés le 19 février 2026), Cegedim santé (données administratives de 15 millions de patients, dont 169 000 annotations médicales sensibles), Agence nationale des titres sécurisés (ANTS) dont plus de 11 millions de comptes auraient été compromis ainsi qu'une série systémique visant les fédérations sportives (UNSS, gymnastique, athlétisme, voile, natation, tennis, chasseurs, etc.), exposant des millions de licenciés. S'y ajoutent des atteintes à répétition contre les collectivités territoriales, des prestataires mutualisés et des éditeurs SaaS qui constituent autant de *hubs* dont une seule compromission expose des millions de profils. Ces fuites de données sont d'autant plus préoccupantes que certaines informations compromises (numéro de sécurité sociale, données biométriques, données de santé, domicile) ne sont, par nature, pas réinitialisables et exposent durablement les victimes au *phishing* ciblé, à l'usurpation d'identité voire, comme l'ont montré plusieurs affaires récentes, à des atteintes physiques (cambriolages ciblés, intimidations...). En conséquence, il souhaiterait savoir quelles mesures concrètes le Gouvernement entend prendre, dans le cadre de la stratégie nationale de cybersécurité 2026-2030, pour imposer aux administrations, opérateurs de services essentiels et prestataires mutualisés un socle minimal de sécurité. Il l'interroge également sur le plan d'appui spécifique prévu pour les collectivités territoriales et les établissements de santé, particulièrement exposés et souvent dépourvus des ressources techniques nécessaires, ainsi que sur l'évolution éventuelle du régime de sanctions et de la responsabilité des responsables de traitement, notamment publics, lorsque des manquements avérés aux obligations du règlement général sur la protection des données (RGPD) sont à l'origine de fuites massives. Il souhaite enfin savoir si le Gouvernement entend instaurer un véritable mécanisme d'indemnisation-sanction à la charge directe des entités défaillantes, permettant aux personnes dont les données ont été compromises d'obtenir, de la part du responsable de traitement lui-même, une réparation forfaitaire et automatique dès lors qu'un manquement à ses obligations de sécurité est à l'origine de la fuite. Un tel dispositif existe, sous différentes formes, dans d'autres pays : dans certains États des États-Unis d'Amérique, les actions collectives conduisent fréquemment les entreprises responsables à verser directement aux personnes concernées des indemnités forfaitaires, indépendamment de tout préjudice financier démontré. En Allemagne, la Cour fédérale de justice juge depuis plusieurs arrêts récents que la seule perte de contrôle sur ses données personnelles constitue, en elle-même, un dommage indemnisable au titre de l'article 82 du RGPD. Au Royaume-Uni, des juridictions ont, en 2025, confirmé l'absence de seuil de gravité pour l'indemnisation au titre de ce même article, dès lors qu'une anxiété ou une crainte objectivement fondée est caractérisée. À ce jour, en France, les victimes doivent engager individuellement une action contentieuse longue et coûteuse, dont l'issue reste aléatoire, tandis que les amendes prononcées par la CNIL alimentent le Trésor public sans bénéficier aux personnes lésées. Il lui

demande en conséquence si le Gouvernement entend soutenir une évolution législative instaurant, à la charge des responsables de traitement et de leurs sous-traitants défaillants, une indemnisation forfaitaire automatique au bénéfice des personnes concernées de telle sorte que la négligence en matière de sécurité, si elle est avérée, ait un coût direct pour celui qui l'a commise et produise une réparation effective pour celui qui la subit.

Données clés

Auteur : M. Thomas Ménagé
Circonscription : Loiret (4e circonscription) - Rassemblement National
Type de question : Question écrite
Numéro de la question : 14767
Rubrique : Sécurité des biens et des personnes
Ministère interrogé : Intelligence artificielle et numérique
Ministère attributaire : Intelligence artificielle et numérique

Date(s) clée(s)

Question publiée au JO le : 28 avril 2026, page 3591