



ASSEMBLÉE NATIONALE

17ème législature

Explosion des violations de données : comment protéger durablement les citoyens

Question écrite n° 14905

Texte de la question

Mme Nathalie Da Conceicao Carvalho interroge M. le ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique sur la progression alarmante de 45 % en un an des violations de données personnelles affectant les citoyens français, tant dans la sphère publique que privée. Le nombre de personnes affectées est désormais estimé à 12,2 millions, tandis que les incidents d'origine intentionnelle progressent de plus de 60 %, portés par la généralisation du *phishing*, le vol d'identifiants et les attaques externes. Le vol de données se présente aujourd'hui comme un phénomène inédit, tant par l'accélération du nombre de fuites recensées que par leur ampleur. Ces vols sont facilités par la dématérialisation des échanges et des données, mais aussi par un accroissement des vulnérabilités lié à une utilisation exponentielle et parfois non maîtrisée des nouvelles technologies, à commencer par la confusion des outils informatiques professionnels et personnels. 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), l'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, tireurs sportifs, chasseurs), exposant des millions de licenciés. S'y ajoutent des atteintes à répétition contre les collectivités territoriales, des hôpitaux, 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 (*homejacking*, cambriolages ciblés, intimidations). Gouverner, c'est prévoir ! Malheureusement, il apparaît ici que la numérisation massive des administrations et des services voulue par l'État semble avoir été très mal anticipée, avec de très graves répercussions potentielles pour les citoyens français. Aussi, elle lui demande quelles mesures le Gouvernement entend prendre pour stopper des fuites massives de données (peut-être en revenant, dans les cas sensibles, aux formulaires papier dans les préfectures, mairies, hôpitaux, ou en supprimant certains fichiers informatiques centralisés afin de limiter les fuites et favoriser la résilience) et s'il entend instaurer un véritable mécanisme d'indemnisation-sanction à la charge directe des entités défailtantes, permettant aux personnes dont les données ont été compromises d'obtenir une réparation forfaitaire et automatique dès lors qu'un manquement à leurs obligations de sécurité est à l'origine de la fuite, comme cela existe déjà, sous différentes formes, dans plusieurs pays.

Données clés

Auteur : [Mme Nathalie Da Conceicao Carvalho](#)

Circonscription : Essonne (2^e circonscription) - Rassemblement National

Type de question : Question écrite

Numéro de la question : 14905

Rubrique : Numérique

Ministère interrogé : [Économie, finances, souveraineté industrielle, énergétique et numérique](#)

Ministère attributaire : [Économie, finances, souveraineté industrielle, énergétique et numérique](#)

Date(s) clé(s)

Question publiée au JO le : [5 mai 2026](#), page 3866