# N° 2734

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 29 avril 2026.

# PROPOSITION DE RÉSOLUTION

*tendant à la création d'une commission d'enquête sur l'***accumulation** *et la* **fuite** *de* **données personnelles** *en France, leurs* **conséquences** *sur les* **libertés publiques** *et les* **responsabilités** *des* **politiques publiques** *en matière de gestion et de* **sécurisation** *des* **données***,*

(Renvoyée à la commission des affaires économiques, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement.)

présentée par

M. Aurélien SAINTOUL, M. Louis BOYARD, M. Ugo BERNALICIS, Mme Mathilde PANOT, Mme Nadège ABOMANGOLI, M. Laurent ALEXANDRE, M. Gabriel AMARD, Mme Ségolène AMIOT, Mme Farida AMRANI, M. Rodrigo ARENAS, M. Raphaël ARNAULT, Mme Anaïs BELOUASSA-CHERIFI, Mme Shéhérazade BENTORKI, M. Christophe BEX, M. Carlos Martens BILONGO, M. Manuel BOMPARD, M. Idir BOUMERTIT, M. Pierre-Yves CADALEN, M. Aymeric CARON, M. Sylvain CARRIÈRE, Mme Gabrielle CATHALA, M. Bérenger CERNON, Mme Sophia CHIKIROU, M. Hadrien CLOUET, M. Éric COQUEREL, M. Jean-François COULOMME, M. Sébastien DELOGU, M. Aly DIOUARA, Mme Alma DUFOUR, Mme Karen ERODI, Mme Mathilde FELD,

M. Emmanuel FERNANDES, Mme Sylvie FERRER, M. Perceval GAILLARD, Mme Clémence GUETTÉ, Mme Zahia HAMDANE, Mme Mathilde HIGNET, M. Andy KERBRAT, M. Bastien LACHAUD, M. Abdelkader LAHMAR, M. Maxime LAISNEY, M. Arnaud LE GALL, M. Antoine LÉAUMENT, Mme Élise LEBOUCHER, M. Aurélien LE COQ, M. Jérôme LEGAVRE, Mme Sarah LEGRAIN, Mme Claire LEJEUNE, Mme Murielle LEPVRAUD, Mme Élisa MARTIN, M. Damien MAUDET, Mme Marianne MAXIMI, Mme Marie MESMEUR, Mme Manon MEUNIER, M. Jean-Philippe NILOR, Mme Sandrine NOSBÉ, Mme Danièle OBONO, Mme Nathalie OZIOL, M. René PILATO, M. François PIQUEMAL, M. Thomas PORTES, M. Loïc PRUD'HOMME, M. Jean-Hugues RATENON, M. Arnaud SAINT-MARTIN, Mme Ersilia SOUDAIS, Mme Anne STAMBACH-TERRENOIR, M. Aurélien TACHÉ, Mme Andrée TAURINYA, M. Matthias TAVEL, Mme Aurélie TROUVÉ, M. Paul VANNIER,

députés et députées.

# EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

Au cours des dernières années, la France a connu une succession continue de cyberattaques ayant conduit à des fuites massives de données personnelles touchant des millions de personnes, ainsi qu'à des coûts économiques considérables. Selon les données publiées par la Commission nationale de l'informatique et des libertés (CNIL), plus de 5 600 violations de données ont été recensées en 2024, soit une augmentation de 20 % en un an, avec une progression continue en 2025. Les autorités publiques reconnaissent elles-mêmes une situation durable, décrite par M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) comme une « marée haute qui perdure ».

En janvier 2024, les opérateurs de tiers payant *Viamedis* et *Almerys* ont été victimes d'une cyberattaque massive, exposant les données de plusieurs millions d'assurés (1). En mars 2024, une attaque contre *France Travail* a conduit à la compromission des données de près de 36 à 43 millions de personnes, incluant des informations collectées sur une période pouvant atteindre vingt ans (2). En octobre 2024, l'opérateur *Free* a subi une fuite concernant près de 19 millions de clients, incluant des données bancaires (3).

En 2025, les incidents se poursuivent. Des fédérations sportives, des entreprises de télécommunications, des opérateurs d'infrastructures numériques ou encore des institutions publiques ont été touchés. Un logiciel médical utilisé par des médecins, développé par *Cegedim*, a été compromis, exposant les données administratives de 15 millions de personnes ainsi que des informations de santé particulièrement sensibles (4).

---

1 Piratage de Viamedis et Almerys : les données de santé plus de 33 millions de personnes concernées, selon la CNIL, *Le Monde* [en ligne], février 2024, disponible à l'adresse : https://www.lemonde.fr/pixels/article/2024/02/07/piratage-de-viamedis-et-almerys-les-donnees-de-plus-de-33-millions-de-personnes-concernees-selon-la-cnil_6215292_4408996.html

2 France Travail : la CNIL enquête sur la fuite de données et donne des conseils pour se protéger, *CNIL,* 13 mars 2024, disponible à l'adresse : https://www.cnil.fr/fr/france-travail-la-cnil-enquete-sur-la-fuite-de-donnees-et-donne-des-conseils-pour-se-proteger

3 PERREAU, Charlie, Free ciblé par une cyberattaque, des données personnelles de clients dérobées, dont des IBAN, *Les Echos* [en ligne], 27 octobre 2024, disponible à l'adresse : https://www.lesechos.fr/tech-medias/hightech/free-cible-par-une-cyberattaque-des-donnees-personnelles-de-clients-derobees-2128072

4 LELOUP, Damien et REYNAUD, Florian, Cegedim : des données personnelles volées à la suite du piratage d'un logiciel pour médecins du groupe, *Le Monde* [en ligne], 27 février 2026, disponible à l'adresse : https://www.lemonde.fr/pixels/article/2026/02/27/des-donnees-de-sante-derobees-a-la-suite-du-piratage-d-un-logiciel-pour-medecins_6668562_4408996.html

La même année, une cyberattaque contre *Bouygues Telecom* a touché 6,4 millions de clients, avec des données comprenant des IBAN et des éléments d'état civil (5). Une intrusion a également concerné l'*Urssaf*, avec un accès frauduleux à des données portant sur environ 12 millions de salariés (6). Le fichier national des comptes bancaires (*Ficoba*) a fait l'objet d'une consultation illégale concernant plus d'un million de personnes (7). Des données issues du ministère de l'Intérieur, notamment du fichier de traitement des antécédents judiciaires (TAJ), ont été consultées à la suite d'une intrusion informatique (8).

Les systèmes concernés reposent sur une collecte massive et centralisée de données personnelles, souvent conservées sur de longues durées, ce qui augmente mécaniquement les risques et l'ampleur des fuites. Le délai entre la publication des vulnérabilités et leur exploitation effective s'est d'ailleurs fortement contracté, une part importante étant exploitée dans la journée, voire dans les heures suivant leur divulgation ; on parle alors de vulnérabilité jour-zéro (9). Les moyens consacrés à la cybersécurité, à la maintenance des systèmes et à la formation des agents apparaissent insuffisants au regard de la sophistication croissante des attaques. La complexité des systèmes d'information et le recours à des prestataires multiples, parfois privés ou étrangers, rendent la sécurisation plus difficile et diluent les responsabilités. La France accuse d'ailleurs un retard préoccupant en matière de souveraineté numérique. Le recours à des prestataires et hébergeurs extra-européens, ainsi que l'absence de stratégie industrielle cohérente dans le domaine de la cybersécurité, fragilisent la protection des données sensibles et exposent celles-ci à des législations

---

5 BOURGIN, Yoann, Bouygues Telecom touché par une cyberattaque, 6,4 millions de clients concernés, *L'usine digitale* [en ligne], 7 août 2025, disponible à l'adresse : https://www.usine-digitale.fr/article/bouygues-telecom-touche-par-une-cyberattaque-6-4-millions-de-clients-concernes.N2236184

6 Accès frauduleux aux données de l'Urssaf : 12 millions de salariés potentiellement concernés, *Le Monde* [en ligne], 19 janvier 2026, disponible à l'adresse : https://www.lemonde.fr/pixels/article/2026/01/19/acces-frauduleux-aux-donnees-de-l-urssaf-12-millions-de-salaries-potentiellement-concernes_6663256_4408996.html#:~:text=L'Urssaf%20a%20lanc%C3%A9%2C%20lundi,de%20salari%C3%A9s%20sont%20potentiellement%20concern%C3%A9s.

7 Les données de 1,2 million de comptes bancaires ont été consultées illégalement depuis la fin de janvier, *Le Monde* [en ligne], 18 février 2026, disponible à l'adresse : https://www.lemonde.fr/pixels/article/2026/02/18/les-donnees-de-1-2-million-de-comptes-bancaires-ont-ete-consultees-illegalement-depuis-la-fin-de-janvier_6667286_4408996.html

8 Cyberattaque contre le ministère de l'intérieur : Laurent Nuñez annonce que « des fichiers importants, dont le traitement des antécédents judiciaires », ont été consultés ; deux enquêtes ouvertes, *Le Monde* [en ligne], 17 décembre 2025, disponible à l'adresse : https://www.lemonde.fr/societe/article/2025/12/17/cyberattaque-contre-le-ministere-de-l-interieur-laurent-nunez-annonce-que-des-fichiers-importants-dont-le-traitement-des-antecedents-judiciaires-ont-ete-consultes-deux-enquetes-ouvertes_6658320_3224.html

9 ANSSI, Panorama de la cybermenace 2025, ANSSI, Paris, 2026, 60p.

étrangères. Enfin, certaines attaques exploitent des failles élémentaires révélant des défaillances organisationnelles plus que technologiques. Près de 80 % des cyberattaques réussies résultent ainsi d'erreurs humaines (10).

Au-delà de ces défaillances, ces incidents invitent à interroger le modèle même de collecte et de conservation des données personnelles. Depuis plusieurs années, une logique d'accumulation massive s'est imposée, tant dans les administrations que dans les entreprises privées, souvent sans que sa nécessité soit systématiquement démontrée. Cette accumulation répond également à des logiques économiques, dans lesquelles la donnée constitue une ressource valorisable, voire un actif stratégique. Dans ce contexte, les fuites ne peuvent être appréhendées comme de simples anomalies, mais comme les conséquences structurelles d'un modèle reposant sur la centralisation et la multiplication des données.

Les conséquences de ces violations de données ne sont pas uniformément réparties. Elles affectent de manière particulièrement aiguë les publics déjà exposés à des formes de précarité économique ou administrative, notamment les demandeurs d'emploi, les bénéficiaires de prestations sociales ou les patients. L'exploitation frauduleuse de leurs données peut entraîner des difficultés accrues d'accès à l'emploi, au logement ou au crédit, renforçant ainsi des inégalités préexistantes. Cette dimension sociale des cyberattaques demeure encore insuffisamment prise en compte dans l'évaluation des risques et des réponses publiques.

Par ailleurs, la circulation des données compromises sur des marchés parallèles ne constitue que le prolongement illégal d'une économie plus large fondée sur la captation, l'agrégation et l'exploitation des informations personnelles. De nombreux acteurs économiques tirent aujourd'hui une valeur significative de ces données, qu'il s'agisse de ciblage commercial, d'analyse comportementale ou d'évaluation des risques. Cette réalité interroge la frontière entre usages légitimes et détournements, et appelle à une réflexion approfondie sur les conditions dans lesquelles les données personnelles peuvent être collectées, exploitées et éventuellement monétisées.

Ainsi, plusieurs interrogations demeurent. Quel est le niveau actuel d'accumulation des données personnelles en France, tant au sein des administrations que des acteurs privés, et comment a-t-il évolué au cours

10 MANACH, Jean-Marc, 80 % des violations de données auraient pu être évitées, déplore la présidente de la CNIL, NEXT [en ligne], 27 janvier 2026, disponible à l'adresse : https://next.ink/221128/80-des-violations-de-donnees-auraient-pu-etre-evitees-deplore-la-presidente-de-la-cnil/

des dernières années ? Quelle est l'ampleur réelle du phénomène des cyberattaques en France : s'agit-il d'une dégradation objective et mesurable de la sécurité des systèmes d'information, ou certaines représentations participent-elles d'une amplification liée à des enjeux d'influence ? Quelle est l'ampleur effective des attaques réellement abouties, au-delà des annonces ou des revendications parfois difficiles à vérifier ? Quelle est la nature exacte et le niveau de sensibilité des données concernées ?

Ces questions préalables conduisent à interroger les conditions de préparation et de réponse des différents acteurs. Les organismes publics et privés sont-ils préparés de manière équivalente face à ces menaces ? Les services de l'État disposent-ils de moyens homogènes et suffisants pour prévenir et détecter ces incidents ? Quels sont les risques concrets encourus par la population, par les institutions publiques et par l'économie nationale ? Enfin, pourquoi, au regard de l'ampleur des enjeux, ces questions ne font-elles pas l'objet d'un débat démocratique approfondi ni de consultations à la hauteur des transformations en cours ?

PROPOSITION DE RÉSOLUTION

## Article unique

① En application des articles 137 et suivants du Règlement de l'Assemblée nationale, il est créé une commission d'enquête de trente membres chargée de :

② 1° Recenser l'ensemble des cyberattaques et fuites de données personnelles ;

③ 2° Faire toute la lumière sur les conditions d'accumulation, de conservation et de sécurisation des données personnelles en France, sur les circonstances et les causes des fuites de données survenues au cours des dernières années ;

④ 3° Déterminer les vulnérabilités en matière de sécurité informatique et de stockage des données personnelles par le service public et les organismes de protection sociale ;

⑤ 4° Étudier le rôle joué par la sous-traitance et l'externalisation dans les pertes ou les vols ou les fuites de données personnelles ;

⑥ 5° Identifier les acteurs à l'origine de cyberattaques, de fuites ou de pertes concernant les données personnelles ;

⑦ 6° Examiner leurs conséquences pour les libertés publiques, la sécurité des personnes et le fonctionnement de l'économie ;

⑧ 7° Élaborer des moyens de prévention, de contrôle et de régulation mis en œuvre par les autorités publiques compétentes, notamment en matière de cybersécurité, afin d'assurer la sûreté des données personnelles et garantir les moyens budgétaires nécessaires pour la pérenniser.