N° 595
SÉNAT

SESSION ORDINAIRE DE 2025-2026

Enregistré à la Présidence du Sénat le 5 mai 2026

PROPOSITION DE RÉSOLUTION

tendant à la **création** *d'une commission d'enquête sur les* **cyberattaques** *et les* **fuites** *de* **données** *portant* **atteinte** *à la* **souveraineté numérique** *de la* **France**,

PRÉSENTÉE

Par Mme Nathalie GOULET, M. Michel CANÉVET, Mmes Sylvie VERMEILLET, Annick BILLON, MM. Michel LAUGIER, Franck DHERSIN, Pascal MARTIN, Olivier HENNO, Mmes Élisabeth DOINEAU, Jocelyne GUIDEZ, Brigitte DEVÉSA, Anne-Catherine LOISIER, M. François BONNEAU, Mme Amel GACQUERRE, MM. Franck MENONVILLE, Claude KERN, Jean-Marie MIZZON, Mme Brigitte BOURGUIGNON, MM. Bernard PILLEFER, Yves BLEUNVEN, Mme Nadia SOLLOGOUB, MM. Pierre-Antoine LEVI, Édouard COURTIAL, Jean-Michel ARNAUD, Mme Catherine MORIN-DESAILLY, M. Jean-François LONGEOT, Mmes Annick JACQUEMET, Christine HERZOG, Marie-Lise HOUSSEAU, MM. Daniel FARGEOT, Laurent LAFON, Patrick CHAUVET, Stéphane DEMILLY, Mmes Évelyne PERROT, Anne-Sophie ROMAGNY, M. Olivier CADIC, Mme Olivia RICHARD, M. Philippe FOLLIOT, Mmes Isabelle FLORENNES, Anne-Sophie PATRU, MM. Vincent CAPO-CANELLAS, Ludovic HAYE, Mme Jocelyne ANTOINE, M. Bernard DELCROS, Mmes Sonia de LA PROVÔTÉ, Anne-Catherine LOISIER, MM. Olivier BITZ et Guislain CAMBIER,

Sénateurs et Sénatrices

(Envoyée à la commission des affaires étrangères, de la défense et des forces armées.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

I. Une vulnérabilité nationale alarmante

La France est désormais le deuxième pays le plus piraté au monde en 2026, et le premier en Europe. Ce constat appelle une réaction immédiate du Sénat. En 2024-2025, le pays a enregistré une progression de 20,6 % des notifications de violations de données auprès de la CNIL, et les données personnelles d'**un Français sur deux** sont aujourd'hui considérées comme exposées.

Ces attaques, qui étaient autrefois principalement orientées vers la perturbation des systèmes, ciblent désormais de manière croissante le vol massif de données personnelles, médicales, financières et stratégiques. Leur coût pour l'économie nationale est estimé à 110 milliards d'euros.

Plusieurs alertes ont déjà été portées sur ce sujet. Dès 2024, le piratage des données de 33 millions de Français par des tiers-payants de santé, puis celui de France Travail — 43 millions de dossiers, la plus grande violation de données personnelles jamais observée en France — avaient mis en évidence les risques considérables de fraude aux prestations sociales et d'usurpation d'identité qui découlent de telles failles. Ces alertes n'ont pas été suivies des mesures nécessaires. Début 2026, le bilan est accablant : plus de 300 services français touchés, 23 millions de comptes compromis, 250 millions de données exposées.

En l'espace de quelques semaines au cours du mois d'avril 2026, plusieurs incidents majeurs ont mis en évidence la gravité de la situation :

• Le 1er avril 2026 : le hacker HexDex a mis en vente 161 343 profils de syndicalistes, incluant leurs données bancaires et personnelles ;

• Le 5 avril 2026 : le groupe DumpSec a revendiqué le piratage de huit agences régionales de santé (ARS), compromettant 35 millions de dossiers médicaux, les données de 130 hôpitaux, ainsi que des données bancaires associées ;

• Le 6 avril 2026 : le groupe Akira a revendiqué le vol de 42 gigaoctets de données internes d'une société du secteur aéronautique, comprenant des documents techniques et des contrats financiers ;

• Le 12 avril 2026 : la plateforme ÉduConnect a été compromise, exposant les données de 3,5 millions d'élèves mineurs et 7,2 millions de bulletins scolaires ;

• Le 15 avril 2026 : l'Agence nationale des titres sécurisés (ANTS) a été piratée, avec 18 à 19 millions d'identités civiles exposées (cartes nationales d'identité, passeports, permis de conduire) ;

• Le 21 avril 2026 : EDF a subi le vol de 93 gigaoctets de documents internes sensibles relatifs aux centrales nucléaires ;

• Le 24 avril 2026 : l'Agence nationale des fréquences (ANFR) a été touchée, exposant les noms, adresses et dates de naissance de 330 000 personnes ;

• Le 24 avril 2026 : l'Agence de services et de paiement (ASP) a été ciblée, avec des données incluant noms, adresses et IBAN ;

• Dans le même temps, une fuite de 40 millions de données de courriels a exposé des entreprises telles que L'Oréal et Renault, ainsi que le réseau diplomatique français ;

• Le système d'information sur les armes a été piraté (62 511 armes), ainsi que la Fédération française de tir et la Fédération nationale des chasseurs.

Le centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) a en outre publié un rapport précisant qu'une cyberattaque peut rester invisible pendant quinze jours, aggravant encore le risque réel pour les victimes.

II. Une dépendance préoccupante à des acteurs extra-européens

Au-delà de la seule question des attaques, la France se trouve dans une situation de dépendance structurelle vis-à-vis de fournisseurs extra-européens, au premier rang desquels Microsoft, qui héberge une part significative des données de l'État et des entreprises françaises. Cette dépendance a été mise en lumière par la récente cyberattaque dont Microsoft a elle-même fait l'objet. La commission d'enquête sénatoriale sur la commande publique (rapport Uzenat-Wattebled, juillet 2025) a relevé que le choix de Microsoft pour héberger le Health Data Hub — la plateforme centralisant les données de santé de millions de Français — constituerait,

selon les termes rapportés lors de ses travaux, une « *erreur caractérisée, si ce n'est une faute politique* ». Le directeur des affaires publiques de Microsoft France, auditionné sous serment par cette même commission, a par ailleurs reconnu ne pouvoir garantir que les données des citoyens français ne seraient jamais transmises à des autorités étrangères.

Plusieurs directives européennes en matière de cybersécurité — notamment la directive NIS2 et la directive sur la résilience des entités critiques (CER) — dont la transposition aurait dû intervenir avant le 17 octobre 2024 ne sont pas encore pleinement transposées et appliquées en droit national. L'arsenal législatif demeure insuffisant face à l'ampleur des menaces.

III. L'insuffisance des réponses apportées à ce jour

Lors de la séance de questions d'actualité au Gouvernement du **8 avril 2026**, le ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique a annoncé la présentation, le lendemain, d'une feuille de route de la sécurité numérique de l'État pour les années 2026-2027. Si cet engagement est bienvenu — *"mieux vaut tard que jamais"* —, il ne saurait suffire.

Les mesures annoncées — fermeture de sites obsolètes, renforcement de l'authentification à double facteur, inscription à l'ordre du jour de l'Assemblée nationale en juillet 2026 du projet de loi relatif à la résilience des infrastructures critiques — constituent des premiers pas, mais ne répondent pas à l'ensemble des questions soulevées par l'ampleur des défaillances constatées.

En particulier, l'état exact de la souveraineté numérique de la France, le périmètre de la dépendance à des prestataires extra-européens, les moyens humains et financiers alloués aux services compétents, ainsi que la cohérence d'ensemble de la politique de cybersécurité nationale restent à évaluer de manière indépendante et exhaustive, avant l'examen du prochain projet de loi de finances.

IV. La nécessité d'une commission d'enquête parlementaire

Des travaux parlementaires ont déjà été conduits sur des sujets proches. En 2024, l'Assemblée nationale a créé une commission d'enquête sur les cyberattaques et fuites de données subies par les organismes de protection sociale, à la suite notamment du piratage de France Travail ayant exposé 43 millions de dossiers. Au Sénat, la dernière commission d'enquête consacrée à la souveraineté numérique remonte à 2019 — soit sept ans —,

ses conclusions étant aujourd'hui largement dépassées par l'évolution de la menace.

Cependant, l'accélération sans précédent des menaces au cours des premiers mois de 2026, la multiplication des incidents touchant simultanément des acteurs publics critiques (ANTS, ARS, EDF, ANFR, ASP), des données ultra-sensibles (identités civiles, données médicales, données nucléaires) et le tissu économique national justifient pleinement la création d'une instance d'investigation dotée des pouvoirs d'enquête les plus larges.

Seul un tel instrument permettra d'évaluer avec rigueur : l'état réel de la sécurisation des systèmes d'information de l'État et des opérateurs d'importance vitale ; le degré de dépendance de la France à des prestataires numériques extra-européens ; l'adéquation des moyens humains, techniques et financiers de l'ANSSI (Agence nationale en matière de cybersécurité et de cyberdéfense) et du CERT-FR ; l'effectivité des sanctions prévues par la loi à l'encontre des auteurs et des utilisateurs de données piratées ; ainsi que les conditions dans lesquelles doit être développé un écosystème souverain d'entreprises françaises et européennes du secteur de la cybersécurité.

Tels sont les motifs pour lesquels il vous est demandé d'adopter la présente proposition de résolution.

Proposition de résolution tendant à la création d'une commission d'enquête sur les cyberattaques et les fuites de données portant atteinte à la souveraineté numérique de la France

Article unique

① En application de l'article 51-2 de la Constitution, de l'article 6 de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires et de l'article 8 *ter* du Règlement du Sénat, est créée une commission d'enquête composée de vingt et un membres, chargée :

② – d'établir un bilan exhaustif des cyberattaques et fuites de données subies par les administrations, les opérateurs d'importance vitale et les entreprises françaises au cours des trois dernières années ;

③ – d'évaluer les capacités de détection, de réponse et de remédiation des services compétents, notamment de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR), et l'adéquation de leurs moyens humains et budgétaires ;

④ – d'apprécier le degré de dépendance de l'État et des opérateurs stratégiques à l'égard de prestataires numériques extra-européens, et de formuler des recommandations pour y remédier, notamment en faveur d'un hébergement souverain des données sensibles ;

⑤ – d'examiner l'état de transposition des directives européennes en matière de cybersécurité (NIS2, CER, DORA) et leur effectivité ;

⑥ – de proposer les évolutions législatives, réglementaires et budgétaires nécessaires pour renforcer la souveraineté numérique de la France et la protection des données de ses citoyens ainsi que pour développer un écosystème d'entreprises françaises et européennes de cybersécurité.