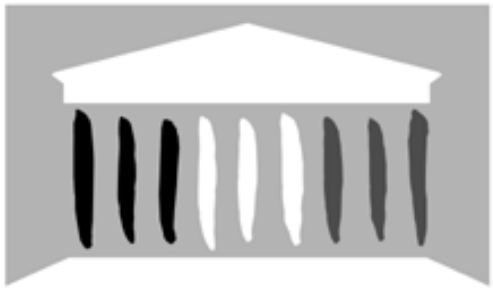

N° 3112

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 27 août 2026.

PROPOSITION DE RÉSOLUTION

tendant à la création d'une commission d'enquête sur les **failles** *de* **cybersécurité** *ayant permis des* **accès**, **fuites** *et* **extractions illégitimes** *des* **données** *confiées par les* **Français** *à l'***État** *et aux* **organismes publics**, *afin d'en identifier les* **causes**, *les* **conséquences** *et les* **responsabilités** *en matière de* **sécurité** *des* **systèmes** *d'***information**,

(Renvoyée à la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement.)

présentée par

M. Philippe LATOMBE,

député.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

L'État et les organismes publics qui agissent pour son compte détiennent, traitent et interconnectent une quantité considérable de données relatives aux citoyens, aux entreprises et aux services publics. Données d'état civil, données fiscales et sociales, informations relatives aux prestations publiques, données de santé, données professionnelles, données relatives aux parcours administratifs, données détenues par les opérateurs et agences de l'État, ces informations constituent un patrimoine informationnel d'une importance majeure, dont la protection relève à la fois de la souveraineté nationale, de la sécurité des citoyens et de la confiance dans l'action publique.

La numérisation croissante des administrations a permis des progrès considérables en matière d'accès aux services publics et de simplification administrative. Elle a toutefois accru la dépendance de l'État à l'égard de systèmes d'information complexes, interconnectés et parfois anciens, ainsi qu'à l'égard de prestataires, sous-traitants et infrastructures techniques, dont la maîtrise et la sécurité doivent pouvoir être garanties dans la durée.

Les incidents de cybersécurité affectant les administrations et les organismes publics ne sauraient dès lors être considérés comme de simples incidents techniques. Lorsqu'une vulnérabilité permet à des personnes non autorisées d'accéder à des données, de les copier, de les exfiltrer, de les modifier ou de les transmettre à des tiers, c'est la sécurité des citoyens et la capacité de l'État à protéger les informations qui lui sont confiées qui sont directement en cause. Les événements récents montrent que ce risque n'est plus théorique et qu'il concerne désormais des administrations placées au cœur des fonctions essentielles de l'État.

Un premier exemple particulièrement significatif est celui du fichier national des comptes bancaires et assimilés (FICOBA). À compter de la fin du mois de janvier 2026, un acteur malveillant ayant usurpé les identifiants d'un fonctionnaire a pu accéder illicitement à une partie de ce fichier, placé sous la responsabilité de la Direction générale des finances publiques (DGFiP). Selon les informations communiquées par le ministère de l'économie et des Finances, l'incident a concerné environ 1,2 million de comptes.

Cet incident présente une caractéristique particulièrement importante pour la présente commission d'enquête : l'accès frauduleux a été rendu

possible par l'usurpation des identifiants d'un agent public disposant d'un accès légitime à la donnée. Il invite donc à examiner les dispositifs d'authentification, la gestion des comptes et des habilitations, les conditions d'accès aux fichiers les plus sensibles ainsi que les mécanismes permettant de détecter qu'un compte légitime est utilisé par une personne non autorisée.

L'enjeu est d'autant plus important que les données concernées, sans permettre à elles seules de connaître le solde ou les opérations réalisées sur un compte bancaire, peuvent être exploitées pour rendre plus crédibles des tentatives d'escroquerie, d'hameçonnage ou d'usurpation d'identité.

L'incident FICOBA a ainsi constitué un premier signal d'alerte concernant la sécurité des données détenues par Bercy. Il est d'autant plus important à examiner qu'une nouvelle série d'accès illégitimes a ensuite affecté, en juin et juillet 2026, le système d'information de la DGFiP. Plusieurs intrusions ont alors conduit à des fuites de données fiscales, cadastrales et successorales concernant plusieurs centaines de milliers de particuliers et de professionnels. La première fuite, révélée en août, concernait environ 350 000 particuliers et portait notamment sur des données fiscales et certains éléments d'échanges avec l'administration. Une deuxième concernait des données cadastrales et pouvait toucher jusqu'à 433 485 particuliers et 1 082 professionnels. Une troisième brèche, liée à un portail relatif aux successions, a également été identifiée.

La gravité de cet épisode tient d'abord à la nature des informations concernées. Les données fiscales susceptibles d'avoir été dérobées peuvent notamment renseigner sur l'identité des contribuables, leur revenu fiscal de référence, leur quotient familial ou leur taux de prélèvement à la source. La DGFiP a toutefois précisé que les intrusions identifiées n'avaient pas permis d'accéder directement aux comptes fiscaux sécurisés des contribuables ni à leurs mots de passe.

Cet épisode soulève surtout une question centrale pour la sécurité numérique de l'État : celle de sa capacité à empêcher non seulement l'intrusion, mais également l'accès anormal aux données et leur extraction. Il impose d'examiner les mécanismes d'authentification, les habilitations, la surveillance des accès, la détection des comportements anormaux, la traçabilité des opérations et la capacité des systèmes à repérer rapidement une extraction inhabituelle de données.

La juxtaposition des affaires FICOBA et DGFiP, à quelques mois d'intervalle, justifie à elle seule un examen approfondi de la chaîne de

sécurité des systèmes d'information financiers de l'État. Dans les deux cas, la question de l'utilisation frauduleuse d'identifiants légitimes apparaît centrale. Dans le second cas, s'ajoute la question de la capacité à détecter suffisamment rapidement l'extraction effective de données.

Le Gouvernement a demandé à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de conduire un audit à la suite des compromissions affectant la DGFiP. Les conclusions de cet audit devront permettre d'établir précisément les circonstances techniques et organisationnelles des incidents. La présente commission devra, sans préjuger de ces conclusions ni des responsabilités individuelles susceptibles d'être établies par les autorités compétentes, pouvoir en examiner les enseignements et déterminer si les mesures correctrices mises en œuvre répondent durablement aux vulnérabilités identifiées.

Un autre exemple particulièrement significatif concerne l'Agence nationale des titres sécurisés (ANTS), devenue France Titres. Le 15 avril dernier, l'agence a détecté un incident de sécurité susceptible d'avoir entraîné la divulgation de données issues de comptes particuliers et professionnels du portail ants.gouv.fr. Selon le ministère de l'Intérieur, 11,7 millions de comptes particuliers étaient susceptibles d'être concernés. Les données potentiellement exposées comprenaient notamment les identifiants de connexion, les noms et prénoms, les adresses électroniques, les dates de naissance et, selon les comptes, les adresses postales, lieux de naissance et numéros de téléphone.

Cet incident est particulièrement préoccupant compte tenu de la nature des services concernés. Le portail de France Titres constitue en effet une porte d'entrée vers des démarches relatives aux cartes nationales d'identité, aux passeports, aux permis de conduire et à l'immatriculation des véhicules. La compromission de données d'identification associées à ces services peut ainsi faciliter des campagnes d'hameçonnage, des tentatives d'usurpation d'identité ou des fraudes administratives, même lorsque les documents eux-mêmes et les données biométriques n'ont pas été exposés.

L'affaire de l'ANTS présente également un intérêt particulier au regard de la gouvernance de la sécurité des systèmes d'information publics. L'incident a été notifié à la Commission nationale de l'informatique et des libertés (CNIL), signalé à l'autorité judiciaire et l'Inspection générale de l'administration a été saisie, afin d'établir les circonstances et la chaîne de responsabilité.

Le ministère de l'Éducation nationale fournit lui aussi plusieurs exemples récents qui appellent un examen approfondi. En avril 2026, le ministère a révélé un incident ayant affecté un service de gestion des comptes des élèves rattaché à ÉduConnect. L'incident trouvait son origine dans l'usurpation, à la fin de l'année 2025, de l'identité d'un personnel habilité. Une faille de sécurité identifiée en décembre 2025 avait été exploitée peu avant sa résolution, permettant à l'attaquant de télécharger des données concernant des élèves au-delà de l'établissement initialement visé. Les informations concernées comprenaient notamment les nom et prénom, l'identifiant ÉduConnect, l'établissement et la classe, ainsi que, lorsqu'elle était renseignée, l'adresse électronique de l'élève.

Cet incident est particulièrement sensible parce qu'il concerne des données relatives à des élèves, dont une grande partie est mineure. Il montre également que la sécurité d'un système d'information public doit être appréciée sur l'ensemble de la chaîne : sécurité des applications, gestion des comptes des personnels habilités, correction des vulnérabilités, contrôle des droits d'accès et capacité à détecter l'utilisation frauduleuse d'un compte pourtant légitime.

En juillet 2026, le ministère de l'Éducation nationale a par ailleurs rendu publique une seconde intrusion frauduleuse, survenue dans la nuit du 25 juillet, visant cette fois le système d'information consacré à la formation des personnels. Là encore, l'accès frauduleux a été réalisé à la suite de l'usurpation d'un compte professionnel. Le ministère a indiqué que cette intrusion avait pu conduire à l'exfiltration de données à caractère personnel concernant un nombre important de ses agents et que le système concerné contenait notamment des éléments d'identité et des informations professionnelles relatives à des agents ayant exercé en académie depuis 2001. Pour une partie d'entre eux, étaient également concernés des coordonnées, une adresse postale, un numéro de téléphone ou un numéro de sécurité sociale. Dès le 26 juillet, le ministère a suspendu l'accès externe au système concerné et activé une cellule de crise.

Ces deux incidents au sein du ministère de l'Éducation nationale présentent un intérêt particulier pour les travaux de la commission : à quelques mois d'intervalle, deux systèmes distincts ont été affectés et, dans les deux cas, l'usurpation d'un compte d'un personnel disposant d'un accès légitime constitue un élément central de l'incident. Ils invitent donc à examiner l'efficacité des dispositifs de double authentification, de gestion des habilitations, de détection des comportements anormaux et de révocation des accès.

Ils soulèvent également une question particulière quant à la protection des données des mineurs et des personnels de l'État. La commission devra notamment vérifier si les systèmes traitant ces données font l'objet d'une classification adaptée aux risques, si les accès sont limités au strict nécessaire et si les dispositifs de surveillance permettent d'identifier rapidement les utilisations anormales des comptes habilités.

La succession de ces incidents est d'autant plus préoccupante qu'elle concerne des fonctions administratives très différentes. Les finances publiques, l'identité et les titres sécurisés, l'éducation, l'emploi et la protection sociale ne reposent pas sur les mêmes applications ni sur les mêmes catégories de données. Leur vulnérabilité successive invite donc à dépasser l'analyse de chaque incident pris isolément, afin d'examiner les éventuelles fragilités communes de la sécurité numérique de l'État.

L'exemple de France Travail est, à cet égard, particulièrement éclairant. En mars 2024, une cyberattaque a été susceptible de concerner les données de 43 millions de personnes, parmi lesquelles des demandeurs d'emploi actuels ou anciens. Les données potentiellement concernées comprenaient notamment des informations d'identification et de contact ainsi que le numéro de sécurité sociale. Cet incident a conduit la CNIL à prononcer en janvier 2026 une sanction de 5 millions d'euros à l'encontre de France Travail pour des manquements relatifs à la sécurité des données.

La multiplication des incidents de grande ampleur est également confirmée par les statistiques de la CNIL. En 2024, celle-ci a reçu 5 629 notifications de violations de données personnelles, soit une progression de 20 % en un an. Le nombre de violations concernant plus d'un million de personnes avait alors doublé par rapport à l'année précédente.

Ces exemples ne permettent pas, à eux seuls, de conclure que les administrations concernées souffriraient toutes des mêmes défaillances. Ils révèlent toutefois un motif récurrent qui justifie une investigation parlementaire : dans plusieurs incidents majeurs, l'attaquant a pu exploiter ou détourner un accès légitime, tandis que la question de la détection des comportements anormaux et de l'extraction des données apparaît également déterminante.

Au-delà de la réalité de chaque incident pris isolément, il convient dès lors de déterminer si les atteintes constatées procèdent de défaillances ponctuelles ou révèlent des fragilités structurelles dans l'organisation et la gouvernance de la cybersécurité de l'État.

Plusieurs questions doivent notamment être examinées : les moyens humains, techniques et budgétaires consacrés à la sécurité des systèmes d'information sont-ils à la hauteur de la sensibilité des données traitées ? Les systèmes les plus critiques font-ils l'objet d'une cartographie exhaustive des risques et de contrôles de sécurité suffisamment réguliers ? Les obligations de sécurité imposées aux opérateurs et prestataires intervenant pour le compte de l'État sont-elles effectivement contrôlées et sanctionnées, lorsqu'elles ne sont pas respectées ?

Il convient également de s'interroger sur la gestion des vulnérabilités et des correctifs de sécurité, sur la segmentation des réseaux, la gestion des habilitations et des comptes à privilèges, la conservation et l'exploitation des journaux de connexion, la détection des comportements anormaux, la sauvegarde des données, ainsi que sur la capacité des administrations à détecter rapidement une intrusion et à en limiter les conséquences.

Les incidents FICOBA, DGFiP et Éducation nationale rendent ces interrogations particulièrement concrètes. La commission devra notamment déterminer si les comptes compromis bénéficiaient de droits d'accès excessifs, si les accès aux données étaient suffisamment segmentés, si les opérations de consultation et d'extraction étaient systématiquement journalisées et analysées et si des mécanismes permettaient de détecter automatiquement des comportements incompatibles avec les fonctions exercées par les comptes concernés.

La question de la gouvernance mérite une attention particulière. La multiplicité des administrations, agences, opérateurs et systèmes d'information peut rendre difficile l'identification d'une responsabilité claire en matière de cybersécurité. Il importe donc d'établir précisément la répartition des compétences entre les administrations concernées, les responsables de la sécurité des systèmes d'information, les directions informatiques, les autorités de contrôle et les différents organismes compétents en matière de cyberdéfense et de protection des données.

La commission d'enquête devra également examiner les conditions dans lesquelles les incidents sont détectés, signalés, documentés et portés à la connaissance des autorités compétentes et, lorsque cela est nécessaire, des personnes concernées.

La question de l'information des citoyens devra faire l'objet d'une attention particulière. La commission devra déterminer si les procédures actuelles permettent d'informer suffisamment rapidement les personnes dont les données ont pu être compromises, mais également si cette

information est suffisamment précise pour leur permettre de prévenir les conséquences concrètes de la fuite.

L'enjeu est d'autant plus important que la compromission d'une donnée administrative ne produit pas nécessairement ses effets immédiatement. Des informations dérobées peuvent être agrégées avec d'autres données provenant d'autres sources, utilisées pour des campagnes d'hameçonnage ciblé, des usurpations d'identité, des fraudes ou des opérations d'influence, voire exploitées dans le cadre d'activités relevant de l'espionnage économique ou de l'ingérence étrangère.

La menace ne se limite d'ailleurs pas à la cybercriminalité motivée par la recherche d'un gain financier. L'ANSSI constate que les intérêts français continuent d'être ciblés par des acteurs étatiques à des fins d'espionnage ou de pré-positionnement. La sécurité des systèmes d'information publics constitue ainsi également un enjeu de souveraineté nationale et de sécurité de l'État.

La commission devra donc établir, autant que possible, l'ampleur des données effectivement exposées ou extraites, la nature des informations concernées, les populations susceptibles d'avoir été affectées, les conséquences financières et opérationnelles pour l'administration, ainsi que les risques encourus par les personnes concernées.

Elle devra également rechercher, pour les incidents relevant de son champ d'investigation, les éventuelles défaillances organisationnelles, techniques, contractuelles ou budgétaires qui ont rendu possibles les accès ou extractions illicites, sans préjuger des responsabilités individuelles ou pénales qui relèvent, le cas échéant, de l'autorité judiciaire.

Cette démarche doit permettre de distinguer les responsabilités relevant de la conception, de l'exploitation, de la maintenance, de la supervision ou de la gouvernance des systèmes d'information, et d'évaluer l'efficacité des dispositifs de prévention et de contrôle mis en place par l'État.

La commission devra également porter une attention particulière à la dépendance de l'administration à l'égard des prestataires, partenaires et organismes disposant d'un accès aux données publiques. Elle devra notamment examiner la nature, l'étendue et la traçabilité des accès accordés à des tiers, les conditions de leur renouvellement et de leur révocation, ainsi que les mécanismes permettant de vérifier que les droits d'accès correspondent effectivement aux fonctions exercées.

Elle devra enfin formuler des propositions concrètes permettant de renforcer durablement la sécurité des systèmes d'information publics. Ces propositions pourront notamment porter sur la gouvernance de la cybersécurité, les moyens humains et budgétaires, les normes de sécurité applicables aux systèmes critiques, les obligations imposées aux prestataires, les procédures d'audit et de contrôle, la détection et la notification des incidents, la protection des données les plus sensibles ainsi que la résilience des infrastructures numériques de l'État.

Il conviendra également d'examiner l'opportunité de renforcer les mécanismes de contrôle parlementaire et d'évaluation régulière de la sécurité des systèmes d'information publics, afin que les enseignements tirés des incidents soient effectivement traduits en mesures correctrices et que leur mise en œuvre puisse être vérifiée dans le temps.

Il ne s'agit donc pas seulement de dresser le bilan des incidents passés. Les compromissions ayant affecté FICOBA et la DGFiP en 2026, l'ANTS et le ministère de l'Éducation nationale en 2026, ainsi que la fuite massive de données ayant concerné France Travail en 2024, montrent que la question posée est désormais celle de la capacité structurelle de l'État à protéger le patrimoine informationnel qui lui est confié.

Ces affaires présentent en effet un point commun essentiel : elles démontrent que la protection des données publiques ne dépend pas uniquement de la sécurité des infrastructures techniques. Elle repose sur une chaîne complète comprenant l'authentification, la gestion des habilitations, la supervision des accès, la détection des comportements anormaux, la capacité d'intervention, la gouvernance des systèmes et l'information des citoyens.

La commission d'enquête devra ainsi déterminer si cette chaîne de sécurité est aujourd'hui suffisamment robuste, homogène et contrôlée, pour garantir aux Français que les données qu'ils confient à la puissance publique sont protégées contre les accès, utilisations et extractions non autorisés, mais également si l'État dispose des moyens nécessaires pour détecter, contenir et traiter rapidement les incidents lorsqu'ils surviennent.

En application de l'article 6 de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires et des articles 137 et suivants du Règlement de l'Assemblée nationale, il appartient au Parlement d'exercer pleinement sa mission de contrôle de l'action du Gouvernement et d'évaluation des politiques publiques.

Tel est l’objet de la présente proposition de résolution.

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 d'examiner les conditions dans lesquelles l'État et les organismes publics placés sous sa tutelle assurent la protection de leurs systèmes d'information et des données qu'ils détiennent, ainsi que les éventuelles défaillances ayant permis des accès, consultations, extractions ou divulgations non autorisés de données.

② La commission d'enquête s'attachera notamment à examiner les circonstances, les causes, les conséquences et la gestion des incidents de cybersécurité ayant affecté récemment des administrations, opérateurs et services publics, notamment ceux concernant le fichier national des comptes bancaires et assimilés, la Direction générale des finances publiques, l'Agence nationale des titres sécurisés devenue France Titres, le ministère de l'Éducation nationale et France Travail, sans que cette énumération soit limitative.

③ Elle évaluera notamment :

④ – L'efficacité des dispositifs d'authentification, d'identification et de gestion des habilitations, notamment lorsque des comptes ou identifiants d'agents publics ont été compromis ou utilisés frauduleusement ;

⑤ – La sécurité des systèmes traitant les données les plus sensibles, notamment les données fiscales, financières, d'état civil, d'identification, de scolarité, de santé, sociales et professionnelles ;

⑥ – La gestion des vulnérabilités et des correctifs de sécurité, ainsi que les délais de détection et de correction des failles ;

⑦ – La capacité des administrations à détecter les comportements anormaux, les accès illicites et les extractions massives de données, notamment au moyen de la journalisation et de l'analyse des traces de connexion ;

⑧ – La segmentation des réseaux et des systèmes d'information, ainsi que la limitation des droits d'accès au strict nécessaire ;

⑨ – Les moyens humains, techniques et budgétaires consacrés à la cybersécurité, leur répartition entre administrations et leur adéquation au niveau de sensibilité des données traitées ;

⑩ – La gouvernance de la cybersécurité de l'État, notamment la répartition des responsabilités entre administrations, opérateurs, directions des systèmes d'information, responsables de la sécurité des systèmes d'information, autorités de contrôle et organismes compétents en matière de cyberdéfense ;

⑪ – Les conditions dans lesquelles les prestataires, sous-traitants et autres tiers accèdent aux systèmes et aux données publics, ainsi que les dispositifs de contrôle, d'audit et de révocation de ces accès ;

⑫ – Les procédures de détection, de signalement, de traitement et de notification des violations de données, ainsi que les conditions dans lesquelles les personnes concernées sont informées ;

⑬ – Les conséquences des incidents pour les citoyens, les agents publics, les entreprises et la continuité des services publics, notamment les risques d'usurpation d'identité, de fraude, d'hameçonnage, d'espionnage économique ou d'ingérence étrangère.

⑭ La commission devra déterminer si les incidents précités relèvent principalement de défaillances ponctuelles propres aux systèmes concernés ou s'ils révèlent des vulnérabilités communes et structurelles dans l'organisation, la gouvernance, la sécurisation et la supervision des systèmes d'information publics.

⑮ Elle formulera, le cas échéant, des propositions visant à renforcer durablement la sécurité et la résilience des systèmes d'information de l'État et des organismes publics, à améliorer la protection des données confiées par les citoyens à la puissance publique et à renforcer les mécanismes de contrôle, d'audit, de prévention et de réaction en matière de cybersécurité.

⑯ La commission d'enquête devra veiller, dans la conduite de ses travaux et la présentation de ses conclusions, à ne pas divulguer les informations dont la révélation serait susceptible de porter atteinte à la sécurité nationale, à la sécurité des systèmes d'information ou à la protection des personnes et des infrastructures critiques.