N° 2513

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

SEIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 12 avril 2024.

PROPOSITION DE RÉSOLUTION

*tendant à la création d'une commission d'enquête sur l'***utilisation** *et la* **protection** *des* **données personnelles** *des* **usagers** *des* **organismes** *de* **protection sociale***,*

(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. Hadrien CLOUET,

député.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

En mars 2024, France Travail et Cap Emploi ont été victimes d'une cyberattaque d'ampleur inédite. Le nom, la date de naissance, les coordonnées postales et téléphoniques ainsi que le numéro de sécurité sociale de 43 millions de personnes ont été subtilisés - soit l'ensemble des inscrits depuis 2004. Il s'agit de la plus grande violation de données personnelles jamais observée en France. La même semaine, plus de huit cent sites internet administratifs de l'État ont été attaqués : le ministère de l'Economie, le ministère de la Culture, le ministère de la Transition Ecologique ou encore la Direction générale de l'aviation civile ont été la cible de cybercriminels. Depuis 2020, les scandales de vols, détournements et fuites de données personnelles dans les services publics et les organismes de protection sociale se multiplient. Pôle emploi, Caisse d'allocations familiales (CAF), Assistance publique – hôpitaux de Paris (AP-HP), laboratoires médicales et opérateurs de tiers payant, collectivités territoriales et collectivités locales en ont été victime de cyberattaque. D'après le *Panorama de la cybermenace 2023* publié par l'Agence nationale de la sécurité des systèmes informatiques (ANSSI), le phénomène s'aggrave depuis 2023 : les cyberattaques à but lucratif ont augmenté de l'ordre de 30 % entre janvier 2022 et juin 2023.

Les conséquences de ces vols de données sont multiples et graves. Des personnes sont dépouillées de leur intimité puis, à partir de cette violence originelle, un ensemble d'usages criminels sont possibles. Via la technique de l'hameçonnage, des escrocs tentent d'obtenir les coordonnées bancaires de leurs victimes à partir des données volées pour effectuer des paiements à leur insu. À partir des informations personnelles volées à la CAF, les pirates peuvent détourner les prestations sociales de leurs cibles en modifiant simplement le relevé d'identité bancaire figurant dans l'espace personnel de l'allocataire. Ces données volées peuvent également se retrouver en vente sur Internet. Ce fut le cas en août 2023, lorsqu'un fichier contenant les données personnelles de plus de 10 millions de demandeurs d'emploi inscrits à Pôle emploi avait été mis en vente sur le *Dark Web* au prix de 900 dollars. Le vol de données personnelles peut avoir des conséquences encore plus dramatiques : l'usurpation d'identité. A partir d'un numéro de sécurité sociale, d'identifiants et de mots de passe des espaces personnels de la CAF ou de la plateforme « impot.gouv », d'une copie d'un permis de conduire ou d'une carte d'identité, les pirates peuvent voler et détruire la vie de leurs victimes. Chaque année en France,

300 000 personnes subissent une usurpation d'identité dont les répercussions peuvent aller jusqu'à la perte du permis de conduire, le surendettement voire l'expulsion. Ces failles béantes dans la cybersécurité des données personnelles sont observées depuis des années mais ne cessent de s'intensifier. Entre février et mars 2024, le nombre de dossiers personnels volés excède le nombre d'habitants de notre pays !

Récapitulons les cas les plus marquants des trois dernières années :

Septembre 2021 : 1,4 million d'individus testés pour un soupçon de covid-19 découvrent la publication de leurs données personnelles sur la plateforme de téléchargement néo-zélandaise MegaUpload. Leurs noms, date de naissance, sexe, numéro de sécurité sociale, coordonnées mail, postale et téléphonique, ainsi que le résultat du test, y demeurent accessibles pendant 5 jours. En cause ? Une négligence dans la suppression des données et une faille liée à l'articulation des logiciels *Dispose,* chargé du transfert de données, et *HCP Anywhere* qui les retient pendant un an sur les serveurs.

Février 2021 : vol des données médicales de 491 840 personnes, en raison d'un défaut de sécurité du logiciel de renseignements médico-administratifs édité par le groupe Dedalus Biologie. Les usagers avaient effectué des prélèvements entre 2015 et 2020 dans une trentaine de laboratoires de biologie médicale du Nord-Ouest de la France. Leurs noms, groupe sanguin, parcours de santé, traitements, pathologies, médecin traitant et mutuelle se retrouvent en accès libre sur Internet.

Juin 2021 : Pôle emploi déclare le piratage du nom, du prénom, des coordonnées postales et téléphoniques, mais également des numéros de permis de conduire d'1,2 millions d'usagers.

Janvier 2023 : la Caisse d'allocations familiales de Gironde reconnaît la mise en ligne en accès libre par un prestataire privé pendant 18 mois d'un fichier comportant des informations personnelles sur 10 024 allocataires. Ce fichier précise le sexe, la date de naissance, la nationalité, l'adresse, la situation professionnelle, le type de logement, le montant du loyer, le statut conjugal, la situation familiale, la nature des allocations, la tutelle, la grossesse ou le handicap le cas échéant, y compris pour les enfants.

Août 2023 : Pôle Emploi admet le vol du nom, du prénom et du numéro de sécurité sociale de 10 millions d'usagers - soit les inscrits des

années 2021 et 2022. Cette perte est due à la vulnérabilité d'un prestataire privé.

Début février 2024, deux plateformes de complémentaires santé opératrices de tiers-payant, Viamedis et Almérus, subissent un piratage d'ampleur. Les données à la fois des assurés et de leur famille, soit 33 millions de personnes, sont ainsi volées. En cause : leur état civil, leur date de naissance, leur numéro de sécurité sociale, leur régime de sécurité sociale et leur mutuelle.

Mi-février 2024 : la CAF subit le piratage de 600 000 comptes d'allocataires via un malware et du phishing. Sont concernés le nom, la composition familiale, la nature, le montant et le calendrier de versement des prestations. Les autorités publiques se terrent deux semaines dans le démenti avant d'admettre ce désastre.

Mars 2024 : France Travail et Cap emploi sont victimes d'une cyberattaque. Le nom, la date de naissance, les coordonnées postales et téléphoniques ainsi que le numéro de sociale de 43 millions de personnes sont subtilisés - soit l'ensemble des inscrits depuis 2004. Il s'agit de la plus grande violation de données personnelles jamais observée en France.

PROPOSITION DE RÉSOLUTION

Article unique

① En application des articles 137 et suivants du Règlement de l'Assemblée nationale, est créée une commission d'enquête de trente membres. Cette commission d'enquête a pour missions :

② 1° de recenser l'ensemble des cyberattaques et fuites de données personnelles qu'ont connu les bénéficiaires de revenus de remplacement, de prestations sociales ou d'un accompagnement par le service public et les organismes de protection sociale ;

③ 2° de déterminer les vulnérabilités en matière de sécurité informatique et de stockage des données personnelles par le service public et les organismes de protection sociale ;

④ 3° d'étudier le rôle joué par la sous-traitance et l'externalisation dans les pertes ou les vols ou les fuites de données personnelles dans le service public et les organismes de protection sociale ;

⑤ 4° d'identifier les acteurs à l'origine de cyberattaques, de fuites ou de pertes concernant les données personnelles dans le service public et les organismes de protection sociale ;

⑥ 5° d'auditionner les responsables publics pour prendre connaissance de leurs réactions à l'égard des pertes, fuites et vols de données personnelles dans le service public et les organismes de protection sociale, ainsi que pour entendre leurs préconisations en la matière ;

⑦ 6° d'émettre des recommandations sur l'action à entreprendre pour assurer la sûreté des données personnelles et les moyens budgétaires nécessaires pour la pérenniser.