N° 2245

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 15 décembre 2025.

PROPOSITION DE RÉSOLUTION

tendant à la création d'une commission d'enquête sur les **dépendances structurelles** *et les* **vulnérabilités systémiques** *dans le* **secteur** *du* **numérique** *et les* **risques** *pour l'***indépendance** *de la* **France***,*

(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

Mme Cyrielle CHATELAIN, M. Pouria AMIRSHAHI, Mme Christine ARRIGHI, Mme Clémentine AUTAIN, Mme Léa BALAGE EL MARIKY, Mme Lisa BELLUCO, M. Karim BEN CHEIKH, M. Benoît BITEAU, M. Arnaud BONNET, M. Nicolas BONNET, M. Alexis CORBIÈRE, M. Hendrik DAVI, M. Emmanuel DUPLESSY, M. Charles FOURNIER, Mme Marie-Charlotte GARIN, M. Damien GIRARD, M. Steevy GUSTAVE, Mme Catherine HERVIEU, M. Jérémie IORDANOFF, Mme Julie LAERNOES, M. Tristan LAHAIS, M. Benjamin LUCAS-LUNDY, Mme Julie OZENNE, M. Sébastien PEYTAVIE, Mme Marie POCHON, M. Jean-Claude RAUX, Mme Sandra REGOL, M. Jean-Louis ROUMÉGAS, Mme Sandrine ROUSSEAU, M. François RUFFIN, Mme Eva SAS, Mme Sabrina

SEBAIHI, Mme Danielle SIMONNET, Mme Sophie TAILLÉ-POLIAN, M. Boris TAVERNIER, M. Nicolas THIERRY, Mme Dominique VOYNET,

députées et députés.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

Le 2 juillet 2024, l'entreprise *Datastream Group* a collecté 380 millions de coordonnées géographiques à travers des applications utilisées au quotidien – Leboncoin, Vinted, Candy Crush… À partir de ces données, ce sont les trajets de 47 millions de personnes qui peuvent être reconstitués.

C'est ce que révèle une enquête journalistique de février 2025, réalisée par neuf médias de référence : Le Monde (France), Bayerischer Rundfunk et Netzpolitik.org (Allemagne), SRF et RTS (Suisse), NRK Beta (Norvège), BNR Nieuwsradio (Pays-Bas), Wired et 404 Media (États-Unis).

L'entreprise *Datastream Group* a transmis à ces journaux, comme elle le fait avec l'ensemble de ses potentiels clients, un échantillon de sa base de données : les données collectées en une journée dans 137 pays. Durant cette journée, les données de 2,5 millions de téléphones ont été captées en Belgique, soit 20 % de la population. En France, un million de numéros de téléphone était présent dans ce fichier, avec de nombreuses informations rattachées. Les journalistes ont pu identifier des personnes en Bretagne, à Bruxelles, à Berlin et ailleurs, retracer les différents événements de leur journée, découvrir des aspects de leur vie intime : leur domicile, leur lieu de travail, leurs visites médicales, leur choix d'application de rencontre, leurs fréquentations de salle de sport, de probables rencontres professionnelles.

Dans la suite de cette enquête, *Le Monde* a indiqué qu'avec les données publicitaires récoltées, il a pu identifier et retracer l'ensemble des trajets de policiers ou militaires français d'élite : identité des gendarmes et policiers en charge de la sécurité du Président de la République Emmanuel Macron, membres du groupe d'intervention de la gendarmerie nationale (GIGN), militaires affectés dans des bases cruciales pour la dissuasion nucléaire, haut responsable de Naval Group…

L'ampleur de cette surveillance est notamment liée à l'existence des courtiers en données, ces entreprises qui collectent, agrègent et revendent ces données. Ces courtiers en données achètent des informations qui ont été trouvées sur les réseaux sociaux, les sites web et les applications, par l'activité en ligne (clics, achats, jeux, pages vues, etc.), par la géolocalisation, mais aussi parfois par les informations stockées par les

services publics. Les courtiers en données vendent ensuite ces informations à d'autres : annonceurs, États ou partis politiques.

La course à la captation des données et leur manipulation ont pris des dimensions menaçantes tant pour nos droits et nos libertés individuelles que pour notre sécurité collective. En effet, cette enquête journalistique confirme les propos de M. Nicolas Lerner, directeur général de la Sécurité extérieure : « *Le téléphone, c'est un espion, c'est un mouchard que vous avez dans votre poche*. »

Cette surveillance de masse et la diffusion de fausses informations constituent un véritable danger pour les régimes démocratiques dans une période de montée des tensions internationales et des régimes autoritaires.

Les États-Unis et la Chine construisent une partie de leur puissance stratégique via les outils numériques. Et la Russie quant à elle utilise les cyberattaques et multiplie les tentatives d'ingérence via les réseaux sociaux. Dans le cadre d'une potentielle guerre hybride, l'enjeu du numérique est donc crucial, plus particulièrement dans une période de remise en cause brutale du multilatéralisme et du droit international.

Les géants du numérique et leur proximité avec les pouvoirs autoritaires.

Plateformes, places de marché, réseaux sociaux, tous ces acteurs sont d'insatiables aspirateurs à données, sans aucune transparence sur leur utilisation et leur revente, et sur leurs liens avec les États dont ils sont originaires, majoritairement les États-Unis et la Chine. En effet, les Américains et les Chinois dominent des secteurs numériques clés : réseaux sociaux (TikTok, X, Meta), intelligence artificielle (ChatGPT…), services cloud (Microsoft Azure, Amazon Web Services…), systèmes d'exploitation (Microsoft), réseau de centres de données (Digital Reality), câbles sous-marins de télécommunications (GAFAM, Huawei…), serveurs informatiques (Foxconn, Dell) et les puces qui les font tourner (Nvidia, Intel, AMD).

Pour la Chine, l'allégeance obligatoire des entreprises au régime gouvernemental est depuis longtemps la norme, ce qui inquiète quant à la probable porosité entre les connaissances des entreprises et celles du pouvoir chinois.

Pour les États-Unis, le *Cloud Act* permet aux autorités américaines d'exiger que les données leur soient fournies. Et, depuis l'élection du

président américain, il y a eu un renforcement autoritaire du pouvoir exécutif, qui s'est accompagné d'une forte collusion de la Maison Blanche avec les patrons de l'industrie numérique américaine.

Si l'illustration la plus forte de cette collusion est l'accession au pouvoir du dirigeant de Tesla aux côtés du Président des États-Unis Donald Trump, plusieurs milliardaires de la Silicon Valley ont prêté allégeance au nouveau Président, qui les a reçus à *Mar-a-Lago*, sa résidence de Floride et de nouveau le 4 septembre dernier lors d'un dîner à la Maison-Blanche. À la tête d'empires technologiques, cette poignée de dirigeants ambitionne non seulement d'étendre sa domination économique, mais également politique, grâce à la manipulation de l'opinion, le contrôle de l'architecture de l'information, l'accaparement des données et la prédation des ressources. Pour cette raison, ils mènent une bataille acharnée contre toute forme de réglementation et garde-fous.

L'Union européenne sur le point d'affaiblir ses protections.

Un cadre législatif légitime et démocratique existe, au niveau français comme au niveau européen. Pendant une décennie, l'Union européenne a été prescriptrice, à l'échelle internationale, d'une régulation inédite, nécessaire et adaptée du numérique : encadrement du marché numérique et lutte contre les pratiques de concurrence déloyale des oligopoles américains (souvent nommés GAFAM) ; règles pour la protection des citoyens face aux dérives nombreuses en matière de désinformation ou de harcèlement ; et combat contre les contenus illicites et dangereux ; protection des données et des droits fondamentaux. Par la taille de son marché et sa capacité réglementaire, l'Europe avait réussi à contraindre partiellement les entreprises opérant sur le plan international à se plier à un cadre juridique exigeant.

Sans surprise, depuis son arrivée au pouvoir, M. Donald Trump a remis en cause les régulations européennes qui limitent le pouvoir des champions américains de la Big Tech. L'administration Trump a mis une pression immense sur la Commission européenne, à travers des menaces publiques et des discussions bilatérales, exerçant un chantage assumé : des tarifs douaniers rédhibitoires et des restrictions à l'exportation sur le continent américain sauf en cas d'affaiblissement important de la législation numérique des 27 États. Dans le même temps, l'industrie de la Tech a dépensé 151 millions pour faire du lobbying au niveau des institutions européennes en 2025 (trois fois plus d'argent que le lobby pharmaceutique ou le lobby automobile) et Huawei, la multinationale chinoise de la tech, est accusée de corruption au Parlement européen.

Au mois de novembre 2025, seulement trois ans après la finalisation de grands textes législatifs, le *Digital Services Act* et le *Digital Markets Act*, et au moment où la Big Tech américaine est la plus offensive, la présidente de la Commission européenne annonce un « omnibus législatif » dérégulateur et moins-disant. La publication de ce paquet législatif semble indiquer un grand retour en arrière sur de nombreux éléments du cadre réglementaire européen, souvent sans étude d'impact préalable. Pourraient être affectés le règlement sur l'intelligence artificielle (IA), le règlement sur l'équité numérique (Data Act), la directive *e-Privacy* (directive vie privée et communications électroniques), et principalement le règlement général sur la protection des données (RGPD). Il est à craindre que cet omnibus entraîne un démantèlement durable des garanties réglementaires, et un recul historique des protections essentielles des citoyens, des enfants, des travailleurs, des minorités.

Dans le même temps, la France et l'Allemagne ont organisé un Sommet sur la Souveraineté numérique européenne à Berlin, où les deux chefs d'État ont insisté sur la nécessité de bâtir une souveraineté numérique de l'Union européenne tout en soutenant la logique de simplification des réglementations européennes. Le processus législatif de détricotage au niveau européen est à son point de départ. Parlement européen et Conseil européen seront maintenant amenés à discuter de ces textes et éventuellement à entériner l'omnibus.

Le rouleau-compresseur américain, les mots d'ordre « simplification » et « compétitivité » sans garde-fous, pourraient avoir raison de la protection des droits des citoyens européens et de la souveraineté des démocraties européennes. Il est donc indispensable de mesurer objectivement et précisément les impacts d'une telle déréglementation.

Des tentatives d'ingérences répétées et de plus en plus fortes.

Deux rapports de 2023, de la délégation parlementaire au renseignement et d'une commission d'enquête ont souligné les fragilités de la France en matière d'ingérences étrangères, « *agressions ou tentatives de déstabilisations protéiformes émanant de l'étranger* ». Ces rapports reconnaissent un niveau élevé de menaces, qui proviennent principalement de Russie, de Chine, de Turquie et d'Iran. De plus en plus, ces tentatives d'ingérences se font à travers les outils numériques. Les cyberattaques deviennent plus fréquentes sur tous les systèmes d'information publics ou qui visent des entreprises privées liées à l'armement et à la stratégie.

Mais à côté de ces cyberattaques, méthodes de tentative de sabotage plus classiques, la guerre hybride prend aussi la forme d'opération d'influence et de manipulation de l'information dans le but d'infléchir l'opinion publique ou des personnalités publiques, et ainsi agir sur les sentiments et les directions prises par le pays. En créant à l'aide de l'IA des vidéos ou des enregistrements audios falsifiés, en générant des posts sur les réseaux sociaux et du contenu de désinformation virale, et en utilisant des bots et des comptes automatisés pour amplifier leurs effets, des États hostiles tentent de créer des divisions dans la société et d'affaiblir sa cohésion ou de créer des doutes quant à la conduite des institutions.

Le service de vigilance et de protection contre les ingérences numériques étrangères a remis un rapport en février 2025 sur la « manipulation d'algorithmes et l'instrumentalisation d'influenceurs » afin de tirer les enseignements de ce qui s'est déroulé lors de l'élection présidentielle en Roumanie, premier scrutin démocratique en Europe à avoir fait l'objet d'une annulation en raison de soupçons d'ingérences étrangères. Dans ces conclusions ce rapport met en lumière « *la relative facilité avec laquelle il est aujourd'hui possible d'imposer aux utilisateurs la visibilité d'un sujet sur un réseau social tel que TikTok, sans que le dispositif utilisé ne soit d'emblée modéré ou considéré comme inauthentique par la plateforme, et d'autre part, le rôle et la vulnérabilité des influenceurs, exposés à un risque croissant d'instrumentalisation de la part d'acteurs malveillants utilisant des approches dissimulées.* »

Alors que le scrutin présidentiel aura lieu en France en 2027, il est indispensable d'estimer la fragilité de notre pays à de telles pratiques d'ingérence et d'établir les outils nécessaires pour les empêcher.

Les données sensibles traitées par l'administration qui peuvent potentiellement être saisies par de nombreux acteurs hors de France

La mainmise de quelques mastodontes du numérique sur le secteur des applications et de la navigation n'est pas notre seule dépendance. Plus de 80 % du total des dépenses liées aux logiciels et services cloud à usage professionnel en Europe est passé auprès d'entreprises américaines. Cette dépendance massive aux prestataires extra-européens se vérifie aussi dans les administrations françaises, notamment vis-à-vis des géants américains du cloud. Près de 70 % des dépenses publiques françaises en infrastructure numérique vont à des entreprises américaines. Cela veut dire pour le citoyen français que des données sensibles sont hébergées sur des serveurs américains, donc soumis aux lois américaines et non européennes, bien plus protectrices.

Le rapport, paru en novembre 2025, de la Cour des comptes sur *Les enjeux de souveraineté des systèmes d'information civils de l'État*, donne des exemples précis et étayés. Il s'agit du programme de gestion dématérialisée des ressources humaines de l'éducation nationale, d'une Plateforme des Données de Santé dédiée à la recherche et comprenant des données de santé primaires de Français et Françaises, ou plus généralement de tout l'écosystème de soin en France dans son fonctionnement courant (mélange de privé et de services publics). Autant d'informations vitales et précieuses de nos concitoyens qui ne sont plus, aujourd'hui, tout à fait sous la protection du droit français.

Cette dépendance à des outils numériques extra-européens pose non seulement la question de l'encadrement de l'utilisation des données stockées, mais également celle de la maîtrise des outils. Par exemple, M. Donald Trump, en raison de désaccords avec les décisions rendues par la Cour pénale internationale, a décidé de sanctionner des magistrats, dont le juge Nicolas Guillou, président de la chambre préliminaire sur la situation de l'État de Palestine, en leur interdisant l'accès à des services numériques américains (Microsoft, Airbnb, Amazon, PayPal, gel des moyens de paiements comme Visa, Mastercard ou Western Union…). La Cour pénale internationale elle-même a fini par rompre son contrat avec Microsoft, le compte mail du procureur Karim Khan ayant été suspendu. En utilisant des services répondant à des législations extra-européennes, l'administration française s'expose au risque de se retrouver dans l'incapacité de faire fonctionner des services indispensables.

L'autonomie et l'indépendance numérique de la France : un enjeu majeur et immédiat.

La souveraineté numérique de la France implique pour la Cour des comptes :

*« une **maîtrise par un État** des technologies numériques et du droit qui leur est applicable, pour **conserver une capacité autonome d'appréciation, de décision et d'action** dans le cyberespace.*

*Elle suppose ainsi de ne pas se faire dicter des choix technologiques structurants par un tiers et que soient **protégées les données** d'une sensibilité particulière des systèmes d'information de l'État. Il s'agit des données qui relèvent de **secrets protégés** par la loi ou qui sont **nécessaires à l'accomplissement des missions essentielles** de l'État et **dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité***

publique, à la santé et à la vie des personnes, ou à la protection de la propriété intellectuelle. »

De même, le contrôle des infrastructures permettant le fonctionnement des outils numériques est un enjeu incontournable pour garantir notre indépendance numérique. Des projets de centre de données portés par des fonds d'investissement américains ou des Émirats arabes unis, se multiplient sur le territoire. Si l'atteinte de l'autonomie technologique est plus longue à atteindre sur le plan matériel des composants, elle ne peut être négligée. La maîtrise des outils numériques et de leurs effets dépend tout autant de celui qui maîtrise les données, que de celui qui maîtrise les infrastructures par lesquelles ces données transitent.

Il est nécessaire de changer de regard sur les législations numériques à mettre en place. À ce stade, le législateur s'est principalement focalisé sur l'encadrement des pratiques des utilisateurs, sans suffisamment réglementer les actions des acteurs du numérique.

L'objectif de cette commission d'enquête est d'étudier nos dépendances et vulnérabilités numériques (infrastructures, logiciels, industriels) et notre capacité d'autonomie (maîtrise technologique, immunité à l'influence étrangère, outils juridiques).

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 :

② 1° d'évaluer la capacité d'autonomie, d'appréciation, de décision et d'action de l'État français et des collectivités territoriales dans le domaine du numérique ;

③ 2° d'évaluer le niveau général d'autonomie et d'indépendance de la France dans le secteur du numérique en termes d'infrastructures, de protection des données ou encore de choix stratégiques structurants ;

④ 3° d'évaluer la dépendance des services de l'État, des services aux publics délivrés par l'État, des structures liées à l'État et des collectivités territoriales, à des services numériques fournis par des acteurs dont le siège est situé hors de France ;

⑤ 4° d'évaluer l'état du développement d'infrastructures numériques, de matériels utilisés dans des outils numériques, de logiciels et de systèmes d'informations fournis par des acteurs publics ou privés français ;

⑥ 5° d'évaluer la capacité de résistance de la France face au risque d'ingérence ;

⑦ 6° de vérifier spécifiquement que toutes les mesures sont prises en termes de protection des données sensibles ;

⑧ 7° d'identifier plus précisément les mécanismes techniques et juridiques qui permettent à des acteurs non français, entreprises privées ou États, d'avoir accès aux données des citoyens sans leur consentement ;

⑨ 8° d'examiner la capacité de l'État français à défendre l'autonomie et l'indépendance numérique de la France dans le cadre de l'omnibus numérique ;

⑩ 9° d'émettre des recommandations pour pallier les éventuelles défaillances institutionnelles et pour accélérer les décisions administratives en vue d'une bien plus grande autonomie et indépendance numérique.