ASSEMBLÉE NATIONALE

17ème législature

Vulnérabilité stratégique de la France face aux données civiles massives

Question écrite n° 12977

Texte de la question

M. Marc Chavent interroge M. le Premier ministre sur l'exposition de la France aux données civiles massives et les mesures de protection envisagées. Les conflits contemporains montrent que la phase initiale d'un affrontement armé est désormais largement informationnelle et statistique, fondée sur la collecte, la corrélation et l'exploitation de données issues de systèmes civils, bien au-delà des seules infrastructures classées d'importance vitale. La France produit quotidiennement, *via* son économie numérique et ses usages grand public, des volumes considérables de données civiles exploitées ou exploitables par des acteurs privés et publics, français ou étrangers. Les applications mobiles de sport, de navigation ou de livraison permettent de déduire des trajets récurrents, des horaires, des zones de résidence et de travail, ainsi que la fréquentation d'infrastructures sensibles, y compris lorsque ces trajets concernent des responsables publics ou des personnels des forces armées et de sécurité, dans un contexte où la CNIL rappelle que les données de connexion et de localisation permettent de reconstituer habitudes de vie, déplacements journaliers et milieux sociaux fréquentés. Les objets de santé connectés et les plateformes de *e-santé* manipulent des données dont la sensibilité et le volume ont déjà conduit à des cyberattaques massives et à des sanctions, comme l'a illustré la fuite de données de centaines de milliers de patients ou la sanction de 380 000 euros prononcée contre un grand site de santé en ligne pour manquements à ses obligations, ce qui confirme la valeur stratégique de ces informations pour des attaquants susceptibles de déduire état de fatigue, stress ou disponibilité opérationnelle d'individus et de catégories professionnelles entières. Les réseaux IoT civils, qu'il s'agisse de capteurs urbains, de compteurs intelligents ou de dispositifs connectés dans les transports, contribuent à une cartographie en temps réel des flux de population et de logistique ; divers travaux sur les réseaux IoT montrent que ces infrastructures permettent d'analyser en temps réel des flux vidéo, audio ou de données environnementales afin d'en déduire comportements collectifs et vulnérabilités, ce qui, corrélé à d'autres métadonnées, peut permettre d'identifier indirectement la localisation et le fonctionnement d'infrastructures critiques. Par ailleurs, le cadre juridique français a déjà reconnu la puissance stratégique des métadonnées : la loi relative au renseignement et les dispositions du code de la sécurité intérieure organisent la collecte des données de connexion, en ce compris la localisation d'équipements terminaux, les listes de numéros appelés et appelants, la durée et la date des communications, précisément parce que ces éléments permettent de reconstituer des réseaux relationnels, des chaînes de commandement et des schémas d'activité sans accéder au contenu des communications. La menace cyber elle-même fait l'objet d'une appréciation consolidée par les autorités compétentes : l'ANSSI décrit une hausse continue des incidents et signalements, notamment dans le cadre des grands évènements comme les jeux Olympiques et souligne que la menace affecte tous les territoires, avec une attention particulière aux systèmes d'information d'importance vitale et aux systèmes d'information d'importance vitale (SIIV) exploités par les opérateurs d'importance vitale dans le cadre du dispositif SAIV. Cette approche demeure néanmoins principalement centrée sur les infrastructures critiques identifiées, alors que les flux massifs de données civiles, non classés en tant que tels, peuvent produire du renseignement militaire par simple corrélation. Dans ce contexte, si la France s'est dotée de dispositifs avancés de cybersécurité, de souveraineté numérique sectorielle (notamment en matière de données de santé et de *cloud* souverain) et de coopération institutionnelle entre CNIL et ANSSI, ces cadres privilégient encore une approche par catégories de données (données à caractère personnel, données de santé, données d'importance vitale) plutôt qu'une approche par effets de corrélation et d'usage en situation de conflit ou de crise hybride. M. le député souhaite donc savoir, en premier lieu, quelle est l'évaluation actuelle des autorités françaises sur le rôle stratégique de ces données civiles massives

(applications mobiles, objets connectés, réseaux IoT, métadonnées) lorsqu'elles sont exploitées par des puissances étrangères ou des acteurs non étatiques et quels scénarios opérationnels (cartographie de points faibles territoriaux, anticipation de mouvements de population, ciblage de campagnes d'influence, préparation de sabotages ou de cyberattaques) sont retenus dans l'analyse gouvernementale. Il souhaite également savoir si les services de renseignement disposent d'une capacité formalisée et identifiée pour analyser et intégrer ces risques dans la planification de la défense, au-delà des dispositifs de collecte de données de connexion déjà encadrés par la loi relative au renseignement et comment cette capacité s'articule avec les travaux de l'ANSSI sur les SIIV, la stratégie nationale de cybersécurité 2026-2030 annoncée par le Gouvernement et les missions de la CNCTR en matière de contrôle des techniques de renseignement. Il l'interroge en outre sur la manière dont l'État distingue juridiquement les données « civiles » des données « stratégiques » dès lors que leur corrélation, parfois simple et réalisée à partir de sources publiques ou commerciales, produit un renseignement d'intérêt militaire ou de sécurité nationale et si une évolution du droit (par exemple par la création d'une catégorie de « données d'intérêt stratégique » ou par l'extension du périmètre des systèmes d'information d'importance vitale) est envisagée pour mieux prendre en compte ces effets de corrélation. Enfin, il souhaite savoir s'il existe une doctrine nationale explicite visant à réduire l'exposition des flux critiques, y compris pour la mobilité et les habitudes numériques des décideurs et des personnels exposés, en matière de choix d'applications, de configuration des terminaux, d'usage de services reposant sur des infrastructures ou des *clouds* extra européens et si le Gouvernement entend renforcer, par des mesures réglementaires, techniques ou de sensibilisation, les obligations de sécurité applicables aux opérateurs économiques qui collectent et traitent ces données civiles massives susceptibles d'être détournées à des fins de renseignement ou de déstabilisation. Dans ce contexte, il souhaiterait savoir quelles actions le Gouvernement entend mettre en place pour reconnaître, encadrer et réduire l'exposition de la France aux risques stratégiques générés par l'exploitation de ces données civiles massives, tant pour la planification de la défense nationale que pour la protection des décideurs, des forces et des infrastructures essentielles.

Données clés

Auteur : M. Marc Chavent
Circonscription : Ain (5e circonscription) - Union des droites pour la République
Type de question : Question écrite
Numéro de la question : 12977
Rubrique : Numérique
Ministère interrogé : Premier ministre
Ministère attributaire : Premier ministre

Date(s) clée(s)

Question publiée au JO le : 17 février 2026, page 1363