

16ème législature

Question N° : 14218	De M. Philippe Latombe (Démocrate (MoDem et Indépendants) - Vendée)	Question écrite
Ministère interrogé > Numérique		Ministère attributaire > Économie, finances, souveraineté industrielle et numérique
Rubrique >numérique	Tête d'analyse >Conséquences de la récente évolution du Patriot Act	Analyse > Conséquences de la récente évolution du Patriot Act.
Question publiée au JO le : 02/01/2024 Réponse publiée au JO le : 16/04/2024 page : 3047 Date de changement d'attribution : 12/01/2024		

Texte de la question

M. Philippe Latombe alerte M. le ministre délégué auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargé du numérique, sur sur la récente évolution du *Patriot Act*. Afin de proroger le *Foreign Intelligence Security Act* (FISA), le *Patriot Act* est soumis à révision tous les quatre ans. À cette occasion, trouvant sa justification dans un contexte international difficile, le congrès américain vient tout juste de voter deux amendements à la section 702 qui, en vertu des lois extraterritoriales américaines, autorisent l'interception de toutes les communications électroniques sur les cross-connect des datacenters de droit états-unien dans le monde. Jusqu'à maintenant, cette section 702 ne portait que sur les opérateurs de communication et de services. La modification de la provision 504 prévoit maintenant l'extension du dispositif à toutes les entreprises en capacité d'interception. Sont donc concernées en France Equinix, Data4 et DRT / Interxion par exemple, qui sont régies par le droit états-unien. Inauguré il y a peu de jours à Bruges en Gironde, le câble sous-marin d'Equinix, baptisé « câble Amitié », - une appellation qui prend toute sa saveur dans ce nouveau contexte-, et qui permet aux informations numériques de circuler en 34 millièmes de seconde entre Le Porge, à 50 kilomètres de Bordeaux, et Lynn, près de Boston, constitue une illustration très concrète du problème qui se pose dorénavant. M. le député souhaite donc savoir ce que cette modification de la législation américaine va changer pour la certification *SecNumCloud* par l'ANSSI, si cette préoccupation est à l'ordre du jour et quelle réaction le gouvernement envisage face à une évolution inquiétante de la législation américaine qui tend un peu plus à fragiliser une souveraineté nationale déjà très mal en point.

Texte de la réponse

Le Gouvernement suit avec attention les développements législatifs en cours aux Etats Unis concernant les amendements déposés en vue de réformer le Foreign Intelligence Security Act (FISA) et d'étendre possiblement son champ d'application. A ce jour, les discussions se poursuivent au Congrès américain, de telle sorte qu'il est difficile de déterminer précisément l'impact d'une proposition législative parmi d'autres, dont l'issue n'est pas encore avérée. Par ailleurs, les amendements auxquels il est fait référence, dont le champ est très large, ne semblent pas concerner exclusivement les fournisseurs de Cloud, de sorte qu'il conviendra d'en apprécier le cas échéant, s'ils devenaient loi, les effets dans leur intégralité, en lien notamment avec les autorités chargées de l'application de la loi de blocage. S'agissant de *SecNumCloud*, la stratégie de cloud de confiance du Gouvernement repose sur la



qualification SecNumCloud délivrée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui garantit un niveau de protection élevé des services qualifiés contre les accès non-autorisés aux données qu'ils hébergent et traitent, notamment via des lois extraterritoriales. A ce jour, il n'est pas envisagé de remettre en cause ce haut niveau d'exigences en matière de cybersécurité. Là encore, l'impact de ce qui n'est pour l'instant que l'une des propositions législatives amendant le FISA devra être pris en compte le cas échéant au regard de l'ensemble des risques qui feront l'objet d'une attention particulière, au premier rang desquels la protection contre les atteintes à l'intégrité des données par le biais de cyberattaques, tout autant que par l'usage du droit extraterritorial de pays tiers sur le territoire français et européen à des fins non autorisées. Ces possibles évolutions du droit américain conservent dès lors toute l'attention du Gouvernement. Enfin, le Gouvernement demeure pleinement mobilisé afin de mieux protéger les données sensibles de nos administrations comme de nos entreprises, comme en témoigne l'actualisation en 2023 de la Circulaire du Premier ministre de 2021 relative à l'usage du cloud de confiance par les administrations pour l'hébergement des données sensibles et le nouvel appel à projet pour le renforcement de l'offre française et européenne de services cloud, dont la publication a été annoncée le vendredi 22 mars aux Journées numériques de Strasbourg.