ASSEMBLÉE NATIONALE

15 janvier 2018

ADAPTATION AU DROIT DE L'UE DANS LE DOMAINE DE LA SÉCURITÉ - (N° 530)

Rejeté

AMENDEMENT

N º CL12

présenté par
M. Bernalicis, Mme Autain, M. Coquerel, M. Corbière, Mme Fiat, M. Lachaud, M. Larive, M. Mélenchon, Mme Obono, Mme Panot, M. Prud'homme, M. Quatennens, M. Ratenon, Mme Ressiguier, Mme Rubin, M. Ruffin et Mme Taurine

---

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 15, insérer l'article suivant:

« Le Gouvernement remet au Parlement, dans un délai de six mois à compter de la promulgation de la présente loi, un rapport évaluant la géographie précise des risques physiques de fuites de données sur l’architecture de l’Internet français, européen et mondial.

« Cette cartographie doit permettre au Parlement et aux citoyens de pouvoir apprécier les risques de fuite de leurs données et les mesures préventives qui ont été prises par la France ainsi que par les États européens par lesquels transitent ces mêmes données ».

EXPOSÉ SOMMAIRE

La cybersécurité pose ici la question, non abordée, tant par la directive que par le projet de loi, de la préservation matérielle et physique de la souveraineté des données européennes et françaises.

Dans le contexte d’encadrement et de réduction des dynamiques de cybersurveillance de masse dans les infrastructures dites « backbones », les modalités de traitement / stockage mais aussi de circulation des paquets de données à travers les treillages internet européens et mondiaux doivent être analysés.

La réponse à la cybersécurité des infrastructures passe en effet nécessairement par une approche spatialisante des infrastructures télécom afin de repérer les points de fuite / « tapping » des données et préserver certains types de données stratégiques de ces chemins vulnérables, encourager la multiplication des chemins de transit alternatifs plutôt que le recours à des « goulets d’étranglement géographiques ».

Grâce au lanceur d'alerte Edward SNOWDEN ont ainsi été révélés différents programmes d'espionnage de masse exécutés sur de grands câbles internet sous-marins mondiaux transitant notamment par le Royaume-Uni (Programme de cybersurveillance de masse du GCHQ "Tempora"

ou les programmes nord-américains mis en oeuvre par la NSA : https://edwardsnowden.com/wp-content/uploads/2013/11/nsa1024.jpg).

Il faut ainsi assumer d’avoir une approche multiscalaire sur les architectures filaires de l’Internet européen / mondial afin d'assurer une réelle protection des données sensibles contre l’espionnage et les fuites.

A cet effet, ce rapport demande à ce que le Parlement soit informé des points faibles des réseaux matériels français et européens en termes de risque d’espionnage / fuite de données.