Parlement européen

Dépendances stratégiques: la souveraineté de l'UE sur les infrastructures de communication menacée

La montée des tensions géopolitiques et le renforcement des dépendances à l'égard des infrastructures numériques appartenant à des fournisseurs étrangers font craindre pour la souveraineté technologique de l'Union européenne. Les services numériques qu'utilisent les citoyens, les entreprises et les gouvernements de l'Union reposent sur les infrastructures de connectivité: câbles sous-marins, technologies mobiles, satellites, etc. L'état de dépendance à l'égard des fournisseurs étrangers qui les mettent à disposition rend nécessaire l'adoption d'une démarche stratégique visant à concilier l'efficacité technologique avec l'intérêt public et la sécurité nationale.

Contexte

Le renforcement de la souveraineté de l'UE dans des secteurs stratégiques, dont celui des technologies, fait partie des priorités de la Commission pour la période 2024-2029. Henna Virkkunen, vice-présidente exécutive chargée de la souveraineté technologique, de la sécurité et de la démocratie, s'est ainsi vu confier la mission d'assurer la souveraineté technologique sur des installations essentielles et d'en renforcer la résilience. Or, l'augmentation du risque d'espionnage par l'introduction de «portes dérobées» logicielles ou matérielles ou le contrôle de plus en plus marqué des échanges sur les réseaux sont des enjeux liés à la maîtrise des câbles sous-marins, des équipements 5G et des infrastructures satellitaires à caractère stratégique. Dans le cadre de l'élaboration d'une proposition législative visant à instaurer un acte législatif sur les réseaux numériques, la Commission a publié un livre blanc où elle analyse les besoins de l'Union en infrastructures numériques. La quasi-totalité des télécommunications internationales (plus de 99 %) transitant par les **câbles sous-marins**, ceux-ci sont jugés d'importance stratégique. Différents articles et rapports ayant accusé des acteurs étrangers de se servir des réseaux de câbles sous-marins pour espionner d'autres pays, la Commission a publié une recommandation esquissant une série de mesures à prendre au niveau national et à l'échelon européen (dont une boîte à outils pour la sécurité des câbles).

La commissaire Virkkunen a constaté que 42 % des **communications 5G** passaient par des équipements radioélectriques de fournisseurs à haut risque. Dans une communication parue en 2023, la Commission, soulignant que les fournisseurs chinois Huawei et ZTE étaient porteurs de risques sensiblement plus élevés que les autres fournisseurs 5G, a estimé que la décision prise par certains États membres de restreindre leur accès aux réseaux 5G ou de les en exclure était justifiée et conforme à la boîte à outils de l'UE pour la cybersécurité de la 5G. La Commission a également demandé à l'Agence de l'Union européenne pour la cybersécurité d'élaborer un schéma européen de certification de cybersécurité candidat pour les réseaux 5G.

La connectivité par **satellite** est de plus en plus importante pour la souveraineté technologique de l'Union, alors que de nombreux opérateurs de télécommunications s'associent à des entreprises de satellites pour élargir leurs services 5G à des zones reculées. Actuellement, l'Union met au point une constellation de satellites à orbite basse pour sécuriser les communications et éviter les dépendances critiques à l'égard d'infrastructures extraeuropéennes. Mais, les États-Unis dominent le marché (Starlink, par ex.) et ont plusieurs années d'avance sur leurs concurrents établis dans l'UE dans le secteur des services par satellites à orbite basse. La Commission devrait publier une proposition de législation spatiale où elle abordera les questions touchant à la cybersécurité des infrastructures spatiales dans leur ensemble.

Les progrès de la **cryptographie quantique** pourraient permettre d'améliorer la sécurité des communications de l'UE. L'initiative EuroQCI pour une infrastructure européenne de communication quantique (EuroQCI) doit permettre de protéger les données sensibles en utilisant la physique quantique

Auteur: Stefano de Luca, Service de recherche pour les députés
PE 767.234 – Février 2025

pour mettre sur pied un réseau terrestre de fibre optique reliant entre eux des sites stratégiques et un système spatial de connectivité sécurisée de l'Union par satellites (IRIS²) d'ici à 2027.

Position du Parlement

À plusieurs reprises, les législateurs européens se sont déclarés favorables à la conquête d'une souveraineté technologique. Le Parlement a invité la Commission à élaborer une stratégie visant à réduire la dépendance de l'Europe à l'égard des technologies de communication étrangères, en particulier celles de la Chine. En 2023, dans une résolution, le Parlement a demandé au Conseil et à la Commission de mettre au point un dispositif contraignant et ambitieux pour la sûreté de la chaîne d'approvisionnement des technologies de l'information et de la communication et d'exclure l'utilisation d'équipements et de logiciels provenant de fabricants établis dans des pays à haut risque, notamment la Chine et la Russie.