# ASSEMBLÉE NATIONALE

5 mai 2023

PROGRAMMATION MILITAIRE 2024-2030 - (N° 1033)

Retiré

# AMENDEMENT

N º CL17

présenté par
Mme Le Hénanff, M. Albertini, M. Alfandari, Mme Bellamy, M. Benoit, Mme Carel, M. Christophe, M. Favennec-Bécot , M. Gernigon, Mme Félicie Gérard, M. Jolivet, M. Kervran, Mme Kochert, M. Lamirault, M. Larsonneur, M. Lemaire, Mme Magnier, M. Marcangeli, Mme Moutchou, M. Patrier-Leitus, M. Plassard, M. Portarrieu, Mme Poussier-Winsback, M. Pradal, Mme Rauch, M. Thiébaut, M. Valletoux, M. Villiers et Mme Violland

---

## ARTICLE ADDITIONNEL

## APRÈS L'ARTICLE 35, insérer l'article suivant:

Après l’article L. 1332-6-4 du code de la défense, il est inséré un article L. 1332-6-4-1 ainsi rédigé :

« *Art. L. 1332-6-4-1.* – Les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et les opérateurs mentionnés à l’article 5 de la loi n° 2018-133 du 26 février 2018 identifient les traitements de données réalisés sous leur autorité et dont la captation par une puissance étrangère, une organisation étrangère ou sous contrôle étranger porterait une possible atteinte aux intérêts fondamentaux de la nation au sens de l’article 410-1 du code pénal. Ces opérateurs tiennent à disposition du Premier ministre la liste des traitements ainsi identifiés.

« Les traitements ainsi identifiés doivent être opérés exclusivement par une ou plusieurs entités dont le siège statutaire, administration centrale ou principal établissement sont établis au sein d’un État membre de l’Union européenne. Ils ne peuvent être confiés en sous-traitance à une société dont le capital social et les droits de vote sont, directement ou indirectement, détenus individuellement à plus de 24 % et collectivement à plus de 39 %, par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d’un État non-membre de l’Union européenne. Ces entités tierces établies hors de l’Union européenne ne doivent pas disposer d’un pouvoir de fait ou de droit de contrôle des décisions du prestataire. Tout recours à des prestataires ultérieurs doit se faire sous les mêmes conditions.

« Les opérateurs visés au premier alinéa s’assurent que les traitements concernés sont réalisés dans des conditions techniques et organisationnelles qui permettent de garantir qu’aucune puissance étrangère, organisation étrangère ou sous contrôle étranger ne soit en capacité de suspendre les traitements, d’en détourner les finalités ou les moyens, ou de contraindre l’opérateur à en modifier les finalités ou les moyens.

« L'autorité nationale de sécurité des systèmes d'information peut notifier aux opérateurs visés au premier alinéa les catégories de traitements pour lesquels le respect des conditions fixées au présent article s'impose. Elle peut, après mise en demeure restée infructueuse, infliger à un opérateur ayant commis un manquement aux obligations définies au présent article une amende dont le montant ne peut excéder 5 % de son chiffre d'affaires annuel moyen constaté au cours des deux exercices précédents.

« Les hauts fonctionnaires mentionnés à l'article R. 1143-1 du code de la défense s'assurent de la connaissance et de la bonne application des présentes dispositions. »

## EXPOSÉ SOMMAIRE

La donnée est souvent considérée comme l'or noir du 21ème siècle, qu'ils s'agissent des données personnelles ou non-personnelles. La création comme la maîtrise de cette richesse est déterminante pour assurer la souveraineté des organisations, tant privées que publiques. Ces données représentent également un enjeu sans précédent pour assurer la sécurité et la défense de la Nation, notamment lorsqu'elles concernent l'activité des organisations stratégiques de la France.

Des directives existent pour aider les organisations à qualifier le niveau de sensibilité de leurs données et ainsi prendre les mesures nécessaires pour les protéger. Mais elles sont encore peu utilisées et beaucoup de décisions prises en matière de services informatiques ne suffisent pas encore à protéger les données, notamment les plus sensibles.

En effet, il est aujourd'hui trop fréquent que les organisations françaises, y compris les celles qui ont été désignées comme « opérateurs d'importance vitales » (OIV) ou « opérateurs de services essentiels » (OSE), aient recours à des services non-européens pour l'hébergement de leurs données, y compris sensibles. Or, certains fournisseurs de cloud non européens sont aujourd'hui soumis à des législations extra territoriale et peuvent être tenus par les autorités étrangères dont ils dépendent, sans en informer leurs clients, de transmettre des données potentiellement stratégiques pour la Nation française et sa défense.

Le présent article vise à faire cesser cette situation qui fait courir un risque important de captation de ces données par des puissances étrangères et porte atteinte aux intérêts fondamentaux du pays.

En vertu de la protection de la sécurité nationale, le présent article vient contraindre les opérateurs d'importance vitale à identifier leurs données « sensibles », c'est-à-dire les traitements de données réalisés sous leur autorité et dont la captation par une puissance étrangère, une organisation étrangère ou sous contrôle étranger porterait une possible atteinte aux intérêts fondamentaux de la nation.

Ensuite, il vient assurer que ces données ne soient pas confiées à des sociétés non européennes ou contrôlées par des Etats non-membres de l'Union européenne. Il s'agit de sociétés dont le capital social et les droits de vote sont, directement ou indirectement, détenus individuellement à plus de 24% et collectivement à plus de 39%, par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un Etat non-membre de l'Union européenne.

L’agence nationale de la sécurité des systèmes d'information délivre aujourd’hui des qualifications qui permettent d’identifier les organisations qui respectent les plus hauts standards de sécurité et qui sont immunisées au droit extracommunautaire.