# ASSEMBLÉE NATIONALE

17 mai 2023

PROGRAMMATION MILITAIRE POUR LES ANNÉES 2024 À 2030 ET PORTANT DIVERSES DISPOSITIONS INTÉRESSANT LA DÉFENSE - (N° 1234)

| | |
|---|---|
| Commission | |
| Gouvernement | |

Tombé

# AMENDEMENT

N º 1738

présenté par
M. Latombe

---

## ARTICLE 35 BIS

I. – À la première phrase de l’alinéa 3, substituer aux mots :

« sur le territoire »

les mots :

« au sein ».

II. – En conséquence, procéder à la même substitution à la fin de la deuxième phrase du même alinéa.

III. – En conséquence, à l’alinéa 4, après le mot :

« capacité »,

insérer le mot :

« juridique ».

IV. – En conséquence, après le même alinéa, insérer l’alinéa suivant :

« Un décret, pris après avis de la Commission nationale de l’informatique et des libertés et du Service de l’information stratégique et de la sécurité économiques, au plus tard six mois à compter de la publication de la présente loi, précise les catégories de traitements pour lesquels le respect des conditions fixées au présent article s’impose. Il prend en compte l’impact qu’aurait une perte de continuité ou de maîtrise des traitements de données sur les intérêts fondamentaux de la nation. »

V. – En conséquence, compléter cet article par l’alinéa suivant :

« Le présent article entre en application le 1er janvier 2025. »

## EXPOSÉ SOMMAIRE

Ceci est un amendement d'appel. Suite à des discussions, notamment avec l'ANSSI, le SGDSN, le gouvernement et des OIV, il est apparu qu'ils souhaitaient des précisions sur la caractérisation des données sensibles et sur le délai d'application du présent article, tout en partageant sa nécessité. Je propose une nouvelle rédaction qui intègre ces préoccupations.

L'exposé des motifs reste inchangé :

La donnée est souvent considérée comme l’or noir du XXIème siècle, qu’il s’agisse 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 », 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.