

ASSEMBLÉE
DE LA
POLYNÉSIE FRANÇAISE

Commission de l'économie, des
finances et du budget

Papeete, le 16 OCT. 2024

N° 109-2024

Document mis
en distribution

Le 16 OCT. 2024

RAPPORT

relatif à l'avis de l'assemblée de la Polynésie française sur le projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier

présenté au nom de la commission de l'économie, des finances et du budget,

par Monsieur le représentant Tevaipaea HOIORE

Monsieur le Président,
Mesdames, Messieurs les représentants,

Par lettre n° 230/DIRAJ du 10 mai 2024, le Haut-commissaire de la République en Polynésie française a soumis pour avis à l'assemblée de la Polynésie française, un projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier.

À titre liminaire, il convient d'abord de préciser qu'en 2006, le dispositif de sécurité des activités d'importance vitale (SAIV), créé en métropole, a été mis en place dans le but d'assurer la protection d'opérateurs (publics ou privés), identifiés comme indispensables pour la continuité d'activité de la Nation, contre tous actes malveillants (terrorisme, sabotage, cyberattaque) et les éventuels risques naturels, technologiques ou sanitaires. Ce sont ainsi les articles L. 1332-1 et suivants du code de la défense métropolitain encadrent la mise en œuvre de ce dispositif, qui compte plus de 300 opérateurs, désignés par l'État, dans 12 secteurs d'activité, chaque secteur étant supervisé par un ministère coordonnateur.

Dès lors, une activité qualifiée « d'importance vitale » concourt à la production et à la distribution de biens ou de services indispensables à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation. Par nature, ces activités sont difficilement substituables ou remplaçables.

On distingue ainsi 12 secteurs d'activités d'importance vitale, répartis en 4 dominantes :

- La dominante humaine : alimentation, gestion de l'eau, santé ;
- La dominante régaliennne : activités civiles, judiciaires et militaires de l'État ;
- La dominante économique : énergie, finances, transports ;
- La dominante technologique : communications électroniques, audiovisuel et information, industrie, espace et recherche.

Les points d'importance vitale (PIV) sont des établissements, ouvrages ou installations qui fournissent les services et biens indispensables à la vie de la Nation. Les opérateurs d'importance vitale (OIV), désignés par le ministre coordonnateur du secteur, proposent eux-mêmes la liste de leurs PIV qui peuvent être, par exemple, des sites de production, des centres de contrôle, des centres informatiques, etc.

Actuellement, le dispositif compte plus de 1500 PIV, répartis sur l'ensemble du territoire national (outre-mer comprises), dont l'identification est protégée par le secret de la défense nationale.

L'objectif du présent projet de loi vise donc à augmenter de manière significative les mesures de protection – avec la mise en place de plans de contingence – pour les activités de ces OIV, fournissant un « service essentiel », au sens de la réglementation européenne.

I- Introduction générale du projet de loi

1. De l'obligation de garantir la sécurité des sites critiques

Désignés par l'État, les OIV sont tenus de garantir à leurs frais la sécurité de leurs sites et de leurs systèmes d'information les plus critiques contre tout risque et toute menace, notamment à caractère terroriste. À travers un certain nombre de documents de planification, les OIV exposent les choix de sécurité leur permettant de répondre à cette obligation de résultat.

Entre autres, ces plans identifient d'abord les PIV concernés, procèdent à une analyse complète de l'ensemble des risques et des menaces pouvant affecter leurs activités et vont même jusqu'à mettre en scénario l'application des mesures Vigipirate qui les concernent. Ces plans démontrent les dispositifs de sécurité et de gestion de crise retenus.

Depuis 2013, le code de la défense impose aux OIV des obligations similaires en termes de cybersécurité, notamment pour leurs « systèmes d'information d'importance vitale » (SIIV). En contrepartie, l'État veille à la bonne application du dispositif, mais surtout accompagne et soutient les OIV, à travers notamment l'évaluation des risques et menaces ou encore par l'imposition de mesures administratives et pénales à l'encontre des OIV qui ne respectaient pas leurs obligations de protection.

2. De la transposition de trois directives européennes

Le présent projet de loi entend principalement transposer trois directives européennes connexes, auxquelles correspondent ses trois titres, et prendre plusieurs dispositions complémentaires dans leurs champs respectifs. Ces directives européennes ont offert un socle minimal commun à tous les opérateurs de l'Union européenne, qui jusque-là, n'étaient pas tous couverts par un dispositif comparable à celui mis en œuvre en France. La transposition s'inscrit ainsi donc dans une politique de résilience globale et cohérente.

a. Titre Ier - Transposition de la directive européenne sur la Résilience des Entités Critiques (REC)¹

Adoptée le 14 décembre 2022, la directive REC est l'aboutissement d'une réflexion européenne, déjà initiée en 2008, dont l'ambition est d'améliorer la fourniture, dans le marché intérieur européen, de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales en renforçant la résilience des opérateurs d'importance vitale, désignés comme « entités critiques ».

Les infrastructures critiques, déjà soumises aux risques naturels, sont régulièrement la cible d'attaques physiques et cyber. Les conflits de haute intensité actifs sur le continent européen et à ses frontières ont mis en lumière la vulnérabilité des infrastructures critiques, qui constituent des cibles prioritaires et stratégiques en cas de conflit. Dès lors, leur destruction peut emporter des conséquences graves en France et dans les États voisins, du fait des interdépendances structurelles de ces sociétés. La recrudescence de ces risques et menaces, et les leçons tirées de la pandémie de COVID-19, notamment en termes de sensibilité des chaînes d'approvisionnement, ont conduit à l'adoption de cette directive européenne.

Cependant, la France met déjà en œuvre le dispositif SAIV depuis 2006. Ainsi, le titre Ier du présent projet de loi vise à transposer la directive REC par le prisme d'une révision de ce dispositif national, en conservant ses principes cardinaux, tout en y intégrant les obligations inédites prévues par la directive et l'extension de son champ d'application à de nouveaux secteurs.

Il est à noter que cette directive a été négociée sous présidence française de l'UE ; les travaux nationaux ont ainsi veillé à ce qu'elle soit conforme avec la vision française.

¹ [Directive \(UE\) 2022/2557](#) du Parlement européen et du Conseil du 14 décembre 2022

b. Titre II - Transposition de la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union² (NIS2)

En réponse à l'évolution rapide et à l'intensification de la menace cyber, la directive européenne (UE) 2022/2555, dite « NIS2 », qui succède à « NIS1 », est entrée en vigueur le 16 janvier 2023. Celle-ci ainsi vise à élever considérablement les standards de cybersécurité à travers l'Union européenne, en élargissant considérablement le champ d'application de la « NIS1 », s'adressant ainsi à un éventail d'industries plus large.

Pour mémoire, la « NIS1 » avait établi les bases d'une cybersécurité renforcée sur un ensemble de secteurs d'activité sur le territoire de l'Union européenne. Les cyber-attaques ne visent plus seulement les acteurs et opérateurs stratégiques mais également l'ensemble du tissu économique et social, affectant un nombre de victimes beaucoup plus élevé, avec des conséquences parfois très dommageables.

Ce faisant, la directive « NIS2 » est plus ambitieuse puisqu'elle détermine des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union et élargit considérablement le périmètre des acteurs et secteurs concernés. Elle anticipe les nouvelles formes d'attaques, passant ainsi d'une approche réactive à une stratégie proactive, engageant une collaboration étendue pour assurer la résilience des infrastructures critiques. Ainsi, les entreprises identifiées par les États membres en tant qu'opérateurs de services essentiels devront prendre des mesures de sécurité appropriées et informer les autorités nationales compétentes des incidents graves.

c. Titre III - Transposition de la directive sur la résilience opérationnelle numérique du secteur financier³

Le 16 janvier 2023, le règlement « DORA » et la directive associée sont entrés en vigueur, après leur adoption par le Conseil de l'Union européenne en novembre 2022. Ce règlement est un cadre réglementaire innovant qui s'attaque aux risques posés par la profonde transformation numérique des services financiers.

En effet, l'utilisation généralisée de systèmes de technologies de l'information et de la communication (TIC), l'interconnexion croissante des réseaux et des infrastructures critiques ainsi que par la multiplication de cyber-attaques, de plus en plus sophistiquées, à l'encontre des acteurs du secteur financier ont nécessité la mise en place de dispositions réglementaires.

Dès lors, les obligations opérationnelles qui s'imposent aux principaux acteurs du secteur financier ont été renforcées. Ce règlement est ainsi complété par une directive du même nom, qui regroupe une série de dispositions techniques, visant à clarifier les obligations.

Elle opère des aménagements de nature technique, en modifiant les références de droit interne relatives aux directives déjà transposées, et apporte des précisions garantissant la clarté et la cohérence juridique pour les entités financières agréées et soumises à une surveillance conformément auxdites directives. La transposition de cette directive entraîne ainsi des modifications d'ordre technique de plusieurs codes.

II. Observations et incidences pour la Polynésie française

Plusieurs observations relatives au présent projet de loi peuvent être émises.

1. Des opérateurs relevant de l'encadrement de l'État ou de la Polynésie française

Conformément aux dispositions de l'article 7 de la loi organique statutaire, « dans les matières qui relèvent de la compétence de l'État, sont applicables en Polynésie française les dispositions législatives et réglementaires qui comportent une mention expresse à cette fin ». De manière dérogatoire, les dispositions prises dans les compétences régaliennes (défense nationale, marchés financiers, etc.) sont applicables de plein droit en Polynésie française.

Les directives européennes faisant l'objet de transposition dans le projet de texte concourent à maintenir les « fonctions sociétales ou d'activités économiques vitales dans le marché intérieur » de l'Union européenne et à limiter les « risques numériques auxquels sont exposées toutes les entités financières ». Ces missions relèvent

² Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022

³ Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022

manifestement de la compétence de l'État. Cependant, les dispositions relevant de la défense nationale étant applicables de plein droit, l'État n'a pas précisé lesquelles s'appliquaient en Polynésie française.

Aussi, les activités d'importance vitale sont définies comme celles qui sont « *indispensables au fonctionnement de l'économie, de la société, à la défense ou à la sécurité de la nation* ». Le projet de texte précise ainsi qu'une infrastructure critique comporte « *tout ou partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système nécessaire à l'exercice d'une activité d'importance vitale ou dont une perturbation pourrait mettre gravement en cause la santé de la population ou l'environnement* ».

Il est à relever qu'aucune mesure d'adaptation n'est prévue pour les outre-mer. Il est aisément compréhensible que les opérateurs indispensables au fonctionnement de l'économie ou de la société nationale soient encadrés par l'État ; toutefois, concernant les opérateurs indispensables à l'économie et à la société polynésienne, une certaine opacité demeure.

Il est à supposer que les opérateurs exploitant des infrastructures susceptibles liées à des matières telles que l'économie, les affaires sociales, la santé ou l'environnement, qui sont pour majorité de la compétence du Pays, relèvent bien de l'encadrement de la Polynésie française. En revanche, les opérateurs polynésiens indispensables à la défense ou à la sécurité publique relèveraient bien de la compétence de l'État.

2. De l'impact du projet de loi sur les entreprises polynésiennes

D'abord, l'État ne fournit pas à la Polynésie française la liste des opérateurs d'importance vitale (OIV) locaux. Or, le présent projet de texte entend faire peser sur eux des frais, diverses obligations, des contrôles et l'application de sanctions.

En l'état actuel, il apparaît ardu d'apprécier les conséquences des dispositions du projet de loi sur les entreprises polynésiennes, qui pourraient éventuellement être concernées, alors même qu'il est possible que des contraintes lourdes et couteuses leur soient opposées.

3. Sur les dispositions relatives aux gestionnaires de crédit et acheteurs de crédits

Le III de l'article 2 du projet de texte complète la transposition de la directive (UE) 2021/2167 relative aux gestionnaires de crédits et acheteurs de crédits. Il introduit les dispositions permettant de garantir que les conditions nécessaires à son agrément soient remplies à tout moment par le gestionnaire de crédits, de mieux encadrer les opérations de changement de contrôle d'un gestionnaire de crédit, de conférer à l'Autorité de contrôle prudentiel et de résolution (ACPR) tous les pouvoirs de contrôle nécessaires pour assurer le respect par le gestionnaire de crédit des dispositions déjà existantes en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme.

Ces dispositions sont étendues à la Polynésie française en application du 12° du III de l'article 2 du projet de loi.

Pour mémoire, la Polynésie française a été saisie d'une demande d'avis sur le projet d'ordonnance⁴ relative aux gestionnaires de crédits et aux acheteurs de crédits, pour lequel l'assemblée de la Polynésie française a émis un avis⁵ défavorable du fait que les gestionnaires de crédits relèveraient non pas du droit bancaire et monétaire, qui est de compétence régaliennne, mais du droit des activités et professions réglementées ou encore du droit des sociétés, qui sont des matières dévolues à la collectivité.

En outre, ledit projet d'ordonnance vise à modifier les dispositions du code monétaire et financier afin de garantir l'attractivité du cadre français de la gestion d'actifs après l'entrée en vigueur du règlement 2023/606 du 15 mars 2023 modifiant le règlement (UE) 2015/760 en ce qui concerne les exigences relatives aux politiques d'investissement et aux conditions de fonctionnement des fonds européens d'investissement à long terme et la définition des actifs éligibles à l'investissement, les obligations en matière de composition et de diversification du portefeuille et l'emprunt de liquidités et d'autres dispositions des statuts des fonds et à transposer ces mesures en Polynésie française.

⁴ [*Ordonnance n° 2023-1139 du 6 décembre 2023 relative aux gestionnaires de crédits et aux acheteurs de crédits, publiée au Journal officiel de la République française*](#)

⁵ [*Avis n° 2024-3 A/APF du 18 janvier 2024*](#)

Ces dispositions relèvent partiellement de la compétence de l'État puisque celles afférentes aux gestionnaires de crédits paraissent, sous réserve de l'interprétation du juge, relever de la compétence de la Polynésie française et donc empiéter sur les compétences de la Polynésie française.

4. Sur l'urgence déclarée

L'État saisit en urgence la Polynésie française d'un projet de loi de 46 pages, assorti d'une étude d'impact de 347 pages. Comme il l'a été rappelé à de nombreuses reprises, les saisines en urgence ne permettent pas une analyse critique sur l'application du texte, ses conséquences en Polynésie française et les éventuelles questions de partage de compétence.

Par ailleurs, l'Etat ne fournit ni la version consolidée des textes concernés (code de la défense, code de la sécurité intérieure, code de la santé publique, code des postes et télécommunication...) ni la liste des opérateurs d'importance vitale, ce qui ne permet pas de mesurer les impacts en Polynésie française.

5. Sur la technique rédactionnelle

Des observations sont à soulever et tendent une fois de plus à s'appliquer au présent projet de texte. Celles-ci rejoignent les réserves et recommandations déjà émises par l'assemblée de la Polynésie française en matière d'intelligibilité du droit.

Il est à nouveau souligné l'importance accrue pour les citoyens d'une collectivité régie par le principe de spécialité législative, de pouvoir consulter des codes consolidés, lisibles et intelligibles. Bien qu'il soit admis que les dispositions de ce projet de loi sont souhaitables, compte tenu de la recrudescence des actes malveillants ou des éventuels risques naturels, technologiques ou sanitaires, nécessitant une vigilance constante et une protection étendue, il est noté qu'à nouveau, l'État ne fournit ni la version consolidée des textes concernés ni la liste des opérateurs d'importance vitale, ce qui ne permet pas de mesurer les impacts en Polynésie française.

Les dispositions introduites dans le code des assurances, le code de la mutualité et le code de la sécurité sociale n'ont pas été étendues en Polynésie française. Celles qui sont introduites dans le code monétaire et financier (CMF), qui prévoient ou précisent des obligations à la charge des opérateurs bancaires et financiers, ont été étendues et relèvent intégralement de la compétence de l'État.

Bien que ces dernières n'appellent pas d'observations particulières, il convient une nouvelle fois de rappeler à l'État qu'à l'issue du travail de modification du CMF, il soit indispensable de fournir et de mettre à jour une version consolidée dudit code, dans sa rédaction applicable en Polynésie française.

De plus, le recours systématique au compteur Lifou pour les modifications des textes et, en particulier du CMF, droit très technique, complexe et soumis à de multiples modifications, rend le droit difficilement intelligible et accessible.

Aussi, il est à nouveau demandé aux autorités de l'État la transmission d'une version consolidée des textes et codes intervenant dans les matières relevant de la compétence de la Polynésie française.

* * * * *

Il est à noter que dans la perspective du dépôt de ce projet de loi, le Sénat avait envisagé la création d'une commission spéciale. Toutefois, compte tenu de la dissolution de l'Assemblée nationale, intervenue le 9 juin 2024, les travaux liés au présent projet de texte avaient été suspendus. Le 15 octobre 2024⁶, ce projet de texte a finalement été présenté au conseil des ministres, au niveau national.

* * * * *

Au regard de ces éléments, la commission de l'économie, des finances et du budget, propose à l'assemblée de la Polynésie française d'émettre un *avis défavorable* au projet de loi présenté.

LE RAPPORTEUR

Tevaipaea HOIORE

^{6 6} [Compte rendu du conseil des ministres du 15 octobre 2024](#)

ASSEMBLÉE
DE LA
POLYNÉSIE FRANÇAISE

AVIS N°

A/APF

DU

sur le projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier

L'ASSEMBLÉE DE LA POLYNÉSIE FRANÇAISE

Vu la loi organique n° 2004-192 du 27 février 2004 modifiée portant statut d'autonomie de la Polynésie française, ensemble la loi n° 2004-193 du 27 février 2004 modifiée complétant le statut d'autonomie de la Polynésie française ;

Vu la lettre n° 230/DIRAJ du 10 mai 2024 du Haut-commissaire de la République en Polynésie française soumettant à l'avis de l'assemblée de la Polynésie française un projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier ;

Vu la lettre n° /2024/APF/SG du portant convocation en séance des représentants à l'assemblée de la Polynésie française ;

Vu le rapport n° du de la commission de l'économie, des finances et du budget ;

Dans sa séance du

ÉMET L'AVIS SUIVANT :

L'assemblée de la Polynésie française a été saisie pour avis du projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle du secteur financier.

Le présent projet de loi entend principalement transposer trois directives européennes connexes, qui concourent à maintenir les fonctions sociétales ou d'activités économiques vitales dans le marché intérieur de l'Union européenne et à limiter les risques numériques auxquels sont exposées toutes les entités financières. Ces missions relèvent manifestement de la compétence de l'État. Cependant, les dispositions relevant de la défense nationale étant applicables de plein droit, l'État n'a pas précisé lesquelles s'appliquaient en Polynésie française.

De plus, bien qu'il soit compréhensible que les opérateurs indispensables au fonctionnement de l'économie ou de la société nationale soient encadrés par l'État, il s'avère que concernant les opérateurs indispensables à l'économie et à la société polynésienne, une certaine opacité quant à leur encadrement demeure.

Ensuite, le projet de texte entend étendre à la Polynésie française des dispositions liées aux gestionnaires de crédits et acheteurs de crédits. Pour mémoire, la Polynésie française a été saisie d'une demande d'avis sur le projet d'ordonnance relative aux gestionnaires de crédits et aux acheteurs de crédits, pour lequel l'assemblée de la Polynésie française a émis un avis défavorable du fait que les gestionnaires de crédits relèveraient non pas du droit bancaire et monétaire, qui est de compétence régaliennne, mais du droit des activités et professions réglementées ou encore du droit des sociétés, qui sont des matières dévolues à la collectivité.

Enfin, des observations sont à nouveau soulevées et tendent une fois de plus à s'appliquer sur la technique rédactionnelle retenue par l'État. Celles-ci rejoignent les réserves et recommandations déjà émises par l'assemblée de la Polynésie française en matière d'intelligibilité du droit.

Bien qu'il soit admis que les dispositions de ce projet de loi sont souhaitables, compte tenu de la recrudescence des actes malveillants (terrorisme, sabotage, cyberattaque) ou des éventuels risques naturels, technologiques ou sanitaires, nécessitant une vigilance constante et une protection étendue, il est noté, qu'à nouveau, l'État ne fournit ni la version consolidée des textes concernés ni la liste des opérateurs d'importance vitale, ce qui ne permet pas de mesurer les impacts en Polynésie française.

Les dispositions introduites dans le code monétaire et financier (CMF), qui prévoient ou précisent des obligations à la charge des opérateurs bancaires et financiers, ont été étendues à la Polynésie française et relèvent intégralement de la compétence de l'État.

Bien que ces dernières n'appellent pas d'observations particulières, il convient une nouvelle fois de rappeler à l'État qu'à l'issue du travail de modification du CMF, il soit indispensable de fournir et de mettre à jour une version consolidée dudit code, dans sa rédaction applicable en Polynésie française. De plus, le recours systématique au compteur Lifou pour les modifications des textes et, en particulier du CMF, droit très technique, complexe et soumis à de multiples modifications, rend le droit difficilement intelligible et accessible.

Aussi, est-il à nouveau demandé aux autorités de l'État la transmission d'une version consolidée des textes et codes intervenant dans les matières relevant de la compétence de la Polynésie française.

Compte tenu de ces éléments, le projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier recueille un *avis défavorable* de l'assemblée de la Polynésie française.

Le présent avis sera publié au *Journal officiel* de la Polynésie française et transmis, accompagné de son rapport de présentation, au Haut-commissaire de la République en Polynésie française, au Président de la Polynésie française, aux Présidents de l'Assemblée nationale et du Sénat et aux parlementaires de la Polynésie française.

La secrétaire,

Odette HOMAI

Le Président,

Antony GEROS