# LA CYBERSECURITE, EXEMPLE TYPIQUE DU PARADOXE DES COMPETENCES DE L'ETAT NON PLEINEMENT DEPLOYEES EN POLYNESIE FRANCAISE

***Hervé Raimana Lallemant-Moe****

*La Directive (UE) 2022/2555, connue sous le nom de "directive NIS 2", vise à renforcer la cybersécurité dans l'Union européenne. Elle sera transposée en droit national et étendue aux Outre-mer, y compris la Polynésie française. La cybersécurité, définie par l'ANSSI, est la capacité d'un système d'information à résister aux cyberattaques qui pourraient compromettre la disponibilité, l'intégrité ou la confidentialité des données. En Polynésie française, la cybersécurité est importante, mais il existe des questions sur le partage des compétences entre l'État et la collectivité d'Outre-mer. La cybersécurité recouvre plusieurs compétences étatiques, notamment la défense nationale et la protection des informations sensibles. Les lois et décrets nationaux, tels que ceux relatifs à la protection des systèmes d'information vitaux et à la cryptographie, s'appliquent en Polynésie française. La Polynésie française ne peut pas agir de manière normative dans les domaines de compétence de l'État, mais elle peut coopérer financièrement dans des domaines présentant un intérêt pour les politiques publiques locales. Cette coopération est facultative et doit respecter les normes établies par l'autorité compétente.*

*The European Union Directive (EU) 2022/2555 aims to strengthen cybersecurity within the European Union. It will be transposed into French national law and extended to the Overseas Territories, including French Polynesia. Cybersecurity, as defined by the French Department of Cybersecurity, is the ability of an information system to withstand cyberattacks that could compromise the availability, integrity,*

* PhD, University of French Polynesia. Chercheur associé au laboratoire Gouvernance et Développement Insulaire (UPF) et au Centre de Droit International (Lyon 3), Conseiller spécial environnement à la Vice-présidence de la Polynésie française.

*or confidentiality of stored, processed, or transmitted data. In French Polynesia, cybersecurity is important, but there are questions regarding jurisdiction between the French State and the Overseas Collectivity. Cybersecurity encompasses several French State competencies, including national defence and the protection of sensitive information. National laws and decrees, such as those related to the protection of vital information systems and cryptography, apply directly in French Polynesia. French Polynesia cannot regulate areas that are within the jurisdiction of the French State, but it can financially cooperate for the benefit of local public policies. This cooperation is optional and must comply with the standards established by the competent authority.*

## *I INTRODUCTION*

A l'aube de la transposition en droit national de la Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148[1] (dite « directive NIS 2 ») et de son extension aux Outre-mer et plus particulièrement à la Polynésie française, il convient de faire le point sur ce secteur, exemple caractéristique de compétences principalement étatiques qui ne sont pas déployées à leur plein potentiel sur le territoire polynésien. Au plan national, la cybersécurité est le résultat d'une pluralité d'actions intégrant des mesures de différente nature et mobilisant un large éventail d'acteurs dont les collectivités territoriales[2].

La cybersécurité est une notion protéiforme et à définitions multiples[3]. La recommandation UIT-T X.1205, approuvée le 18 avril 2008 de l'Union internationale des télécommunications[4] dispose qu'elle est:

> l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyber

1 Julie Tamba « La transposition de la directive NIS 2 en droit français : où en est-on et où en êtes-vous? », Dalloz IP/IT, n° 98, 20 février 2025.

2 Giorgia Macilotti « Les collectivités territoriales face à la cybercriminalité : enjeux conceptuels et réflexions sur l'état de la menace », La Semaine Juridique Administrations et Collectivités territoriales n° 21, 27 mai 2024.

3 Rémy Daudigny « Cybersécurité: vers un continuum de la sécurité numérique », La Semaine Juridique Administrations et Collectivités territoriales n° 21, 2147, 27 mai 2024.

4 En matière de télécommunications et de lien entre 5G et cybersécurité, v. Philippe ACHILLEAS, « Un an de droit des communications électroniques », Communication Commerce électronique n° 5, mai 2020.

> environnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyber environnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyber environnement.

En droit de l'Union européenne, l'article 2, 1) du règlement (UE) 2019/881 du 17 avril 2019 « Cybersecurity Act »[5], définit la cybersécurité comme:

> les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces », une cybermenace étant définie comme : « toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes.

Enfin, pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[6], la cybersécurité est un:

> état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

La Polynésie française n'est évidemment pas à l'abri d'attaque sur les systèmes d'information qu'elle héberge[7] et les politiques publiques en la matière sont donc d'importance. Subsiste cependant l'éternelle question du partage de compétence entre l'État et la collectivité d'Outre-mer en la matière.

---

5 Laurence Idot « Communications électroniques - Union européenne, cybersécurité et cyberdéfense: des avancées », Europe n° 12, Décembre 2022.

6 Sébastien Saunier « La cybersécurité, un nouvel objet du droit administratif », La Semaine Juridique Administrations et Collectivités territoriales n° 21, 27 mai 2024.

7 « Cybersécurité: La Polynésie n'est pas à l'abri », Tahiti Infos, 29 août 2022.

Nous examinerons rapidement le fait que la cybersécurité est bien une compétence de l'État (II) dans laquelle la Polynésie française peut potentiellement s'impliquer (III).

## *II LA CYBERSECURITE, UNE COMPETENCE MANIFESTEMENT ETATIQUE*

La cybersécurité est un domaine cadre, qui recoupe différentes compétences ressortissantes à l'État, ainsi que différentes matières sectorielles juridiques. Ces différents éléments relèvent de compétences décrites à l'article 14 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie française[8]. En matière de "cybersécurité" sont directement concernés les compétences relatives à la garantie des libertés publiques (2°), à la défense (4°), les liaisons et communications gouvernementales de défense ou de sécurité en matière de postes et télécommunications (4°), la sécurité et ordre publics (6°), la réglementation des fréquences radioélectriques (6°), le crédit (7°), les règles relatives à son administration (10°) et la communication audiovisuelle (12°).

La protection du secret de la défense relève de la compétence directe de l'État en matière de défense nationale (sans nécessité de respect des règles de spécialité législative) comme le précise l'article 7 de la loi organique statutaire de 2004. A ce propos, l'article L. 2321-1 du Code de la défense prévoit que:

> Dans le cadre de la stratégie de sécurité nationale et de la politique de défense, le Premier ministre définit la politique et coordonne l'action Gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information qui assure la fonction d'autorité nationale de défense des systèmes d'information.

La protection de l'information sensible et diffusion restreinte est aussi assimilable à la défense nationale et relève de la compétence de l'État. Le décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation est ainsi applicable sur l'ensemble du territoire de la République (art. 3);

Sur la sécurité des systèmes d'information d'importance vitale (SIIV) mis en œuvre par les opérateurs d'importance vitale (OIV), des systèmes d'information essentiels (SIE) mis en œuvre par les opérateurs de services essentiels (OSE) ainsi que les obligations pesant sur les fournisseurs de services numériques (FSN)[9], ces

8 Alain Moyrand et Hervé Raimana Lallemant-Moe, Mémento – Introduction à l'étude des institutions politiques et administratives de la Polynésie française (3e éd, éd. CREAPRINT, 2024).

9 Fabrice Mattatia « Vers un smart Pearl Harbor », Revue pratique de la prospective et de l'innovation n° 2, Octobre 2019.

domaines relèvent à l'identique de la compétence de l'État en matière de défense nationale. Le code de la défense est globalement applicable en Polynésie française, à l'exception des dispositions précisées aux articles L. 6311-1 à L. 6316-2 du code précité). Le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information est aussi applicable en Polynésie française (art. 25).

La protection des systèmes d'information de l'État s'applique évidemment aux services et établissements publics de l'État en Polynésie française que ce soit pour le décret n° 2019-1088 du 25 octobre 2019 modifié relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique ou le décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics.

Concernant la détection, l'article L.33-14 du code des postes et communications électroniques (CPCE) qui encadre la possibilité pour les opérateurs de communications électroniques (OCE) de mettre en œuvre des dispositifs de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés et permet à l'ANSSI de s'appuyer sur ces capacités est applicable en Polynésie française à l'instar des possibilités d'alerte aux abonnés des OCE (art. L. 33-15 du Code national des postes et des communications électroniques). La caractérisation des menaces ressortit à l'article L. 2321-2-1 du code de la défense et est applicable en Polynésie française.

En matière de contrôles réglementaires sur la cryptographie, les articles dédiés (30 à 36) de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique[10] s'appliquent en Polynésie française (art. 57).

* * *

Si les principales composantes de la cybersécurité semblent principalement relever de la compétence de l'État en Polynésie française, cela n'empêche pas dans l'absolu la collectivité territoriale d'intervenir dans le domaine. Cette situation doit cependant rester marginale car elle conduit à un abandon d'une compétence et de son déploiement par la République française.

10 Bertrand Colin « Les enjeux des nouvelles technologies de l'information et de la communication sur la protection de la vie privée », Justice et Cassation, 2006, p.48.

## *III UNE POSSIBILITE D'INTERVENTION LOCALE DEVANT RESTER FACULTATIVE*

Pour rappel, il est pour la Polynésie française (ou les communes de la Polynésie française) impossible d'agir normativement dans les domaines ressortissants à la compétence de l'État, principalement décrits à l'article 14 de la loi organique statutaire de 2004. L'article 31 de la loi organique statutaire de 2004 précise cependant que:

> Les institutions de la Polynésie française sont habilitées, dans le respect des garanties accordées sur l'ensemble du territoire national pour l'exercice des libertés publiques, sous le contrôle de l'Etat, à participer à l'exercice des compétences qu'il conserve dans le domaine législatif et réglementaire en application de l'article 14

mais pour un ensemble de compétences spécifiquement identifiés. Les matières susmentionnées en matière de cybersécurité ne font pas partie de cette liste.

Dans la continuité du traditionnel principe d'incompétence négative, il s'infère d'un avis du conseil d'Etat, que l'État ne peut pas confier unilatéralement l'une de ses compétences à la Polynésie française (Avis n° 404232 du 7 décembre 2021). En matière de cybersécurité, le droit national est donc largement applicable et la Polynésie française ne peut agir de manière normative que sur des aspects bien précis relevant directement de sa compétence, à déterminer au cas par cas (par exemple en ce qui concernerait son administration).

Indépendamment des aspects normatifs, il est théoriquement possible en matière de coopération de prévoir une participation financière de la Polynésie française dans un domaine qui échappe à sa compétence normative, mais qui présente potentiellement un intérêt pour une politique publique particulière. Dans une décision du 23 mars 2004, le Conseil d'État avait d'ailleurs précisé à propos du secteur des relations internationales (compétence détenue par l'État) que la Polynésie française était compétente pour décider, par une délibération de son assemblée territoriale, de l'octroi d'une aide humanitaire d'urgence en faveur de populations étrangères, dès lors que la décision d'aider ces populations, d'une part, n'empiète pas sur les orientations de la politique extérieure de la France et d'autre part, se justifie par l'urgence de cette intervention et présente un caractère non permanent[11]. La participation et les actions de la collectivité devront cependant s'inscrire dans le respect des normes produites par l'autorité compétente et applicable au secteur.

Par principe, cette possibilité de coopération est totalement facultative, au sens où c'est à l'autorité compétente de prendre entièrement en charge cette politique

11 Avis rendu par Conseil d'Etat, 10ème et 9ème sous-sections réunies, 24-03-2004, n° 261797.

publique, cette dernière maîtrisant tous les aspects du secteur. Il revient en effet à chaque entité de réglementer la matière relevant de sa compétence et de prendre en charge l'exercice effectif de cette compétence. Les initiatives de la Polynésie française dans un secteur où elle n'est pas directement compétente doivent ainsi s'inscrire dans un besoin identifié de développer localement une politique publique. Cela peut s'expliquer par la défaillance de l'État ou tout simplement dans l'objectif d'aider à la mise en œuvre d'une telle politique par les externalités positives (développement économique, sécurité, *etc.*) que cette dernière peut avoir pour la collectivité.

Dans d'autres cas, les normes nationales obligent les acteurs locaux à mettre en place plus activement certains processus. Pour ce point, il est possible de citer l'exemple du Règlement Général sur la Protection des Données (RGPD) ressortissant aux compétences de l'État, mais qui a obligé la Polynésie française à devenir *compliant* avec ce nouveau régime juridique et à mettre en place un *data protection officer* (DPO) pour son administration, à l'instar des DPO mis en place par toutes les autres personnes morales (acteurs économiques notamment)[12].

En matière de cybersécurité, il convient de s'interroger sur une coopération avec l'ANSSI. Comme rappelé par le Haut-commissaire de la République le 2 février 2024 dans son discours d'ouverture au premier forum de la cybersécurité en Polynésie française[13], l'ANSSI est l'autorité nationale en matière de cybersécurité. Sa mission est de comprendre, prévenir et répondre au risque cyber. Le décret n° 2009-834 du 7 juillet 2009 créant l'Agence nationale de la sécurité des systèmes d'information donne à cette agence, en plus de la sécurité des systèmes d'informations de l'État, une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale, ainsi que celle de contribuer à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion.

La coopération entre l'État et la Polynésie française est ainsi encadrée par la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie française. Ainsi, l'article 168 de la loi organique susmentionnée dispose que:

---

12 Ludovic Pailler « Le paradoxe de la compliance dans le droit de la protection des données », Cahiers de droit de l'entreprise n° 1, Janvier-Février 2025.

13 « Avec Cyberfenua, le Pays et le Haussariat s'emparent du thème de la cybersécurité », Radio 1 Tahiti, 20 février 2024.

> La coordination entre l'action des services de l'Etat et ceux de la Polynésie française est assurée conjointement par le haut-commissaire et le président de la Polynésie française. / Le haut-commissaire et le président de la Polynésie française signent, au nom, respectivement, de l'Etat et de la Polynésie française, les conventions mentionnées aux premier et deuxièmes alinéas de l'article 169 et à l'article 170.

La combinaison des dispositions relative à cette coopération, ainsi que les nécessités procédurales des conventions de coopération/partenariat avec d'autres services et organismes de l'État sont décrites plus en détail dans la circulaire n° 08020/PR du 8 novembre 2019.

***

Si la cybersécurité est en enjeu majeur pour les collectivités territoriales, y compris dans les Outre-mer et pour la Polynésie française, la répartition des compétences dans la loi organique statutaire de 2004 ne laisse que peu de doute sur l'autorité qui doit principalement prendre en charge cette mission. Si la Polynésie française peut totalement accompagner le mouvement, les politiques de cybersécurité doivent être principalement mis en œuvre par la République française. Si l'incapacité de l'État a pleinement déployer certaines de ses compétences dans ses collectivités les plus lointaines persiste, cet élément devra être bien pris en compte dans les potentielles ultérieures modifications de la loi organique statutaire de la Polynésie française.