ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Jeudi 15 mai 2025
Séance de 9 heures 30

Compte rendu n° 4

SESSION ORDINAIRE DE 2024 - 2025

Présidence de M. Philippe Latombe, *Président*

La séance est ouverte à neuf heures trente-cinq.

La commission spéciale a organisé une table ronde d'associations d'élus, avec la participation de M. Michel Sauvade, co-président de la commission numérique nationale (AMF) ; Mme Constance Nebbula, vice-présidente de la Région Pays de la Loire en charge du numérique et de l'intelligence artificielle et M. Alexandre Ventadour, conseiller territorial de Martinique, chargé du numérique et du développement économique (Régions de France) ; Mme Marlène Le Dieu De Ville, vice-présidente en charge du numérique à Intercommunalités de France.

M. le président Philippe Latombe. Mes chers collègues, nous reprenons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité avec une table ronde consacrée à un sujet central : la cybersécurité des collectivités territoriales.

Nous avons souhaité entendre les représentants des différents niveaux de collectivités pour plusieurs raisons. La première tient à la vulnérabilité numérique de nos services publics locaux. La troisième étude 2024 de Cybermalveillance.gouv.fr sur la maturité cyber des collectivités de moins de 25 000 habitants montre qu'une collectivité sur dix déclare avoir été victime d'une ou plusieurs attaques au cours de l'année dernière, l'hameçonnage étant la cause principale dans 30 % des cas. Les conséquences pour les collectivités sont lourdes : interruption de service, destruction, vol de données, pertes financières.

Mais ce sont les usagers qui en subissent les effets : suspension des inscriptions ou des paiements en ligne pour la cantine scolaire, retard dans le versement d'allocations par les centres d'action sociale. En dépit de ces éléments, l'étude montre que 44 % des communes touchées se considèrent faiblement exposées au risque et que 18 % ne savent pas comment évaluer leur niveau d'exposition. Dans ce contexte, votre retour d'expérience nous est particulièrement précieux pour déterminer quel niveau d'obligation inscrire dans la loi et où placer le curseur.

La seconde raison de cette table ronde est liée à l'objet même du texte que nous examinons. Ce projet de loi vise à renforcer la cybersécurité des collectivités dans le cadre de la transposition de la directive européenne NIS 2 (*Network and Information Security 2*), qui établit un niveau commun de cybersécurité dans toute l'Union européenne (UE).

L'article 8 du projet de loi qualifie d'entités essentielles les régions, les départements, les communes de plus 30 000 habitants, ainsi que leurs établissements publics administratifs (EPA) lorsqu'ils exercent des activités relevant de secteurs hautement critiques ou critiques, les communautés urbaines, les communautés d'agglomération comprenant au moins une commune de plus de 30 000 habitants et les métropoles, leurs EPA, lorsqu'ils exercent des activités relevant de secteurs hautement critiques ou critiques. L'article 9 qualifie d'entités importantes les communautés d'agglomération ne comprenant pas au moins une commune de plus de 30 000 habitants, les communautés de communes et leurs EPA dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques.

L'article 14 du projet de loi prévoit que les entités qui ont été qualifiées d'essentielles ou d'importantes doivent mettre en œuvre un certain nombre de mesures techniques, opérationnelles et organisationnelles, pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent, ainsi que pour éliminer –

ou à tout le moins réduire – les conséquences que les incidents engendrent sur les destinataires de leurs services.

Nous avons le plaisir d'accueillir aujourd'hui M. Michel Sauvade, vice-président du conseil départemental du Puy-de-Dôme, maire de Marsac-en-Livradois, qui représente l'association des maires de France et des présidents d'intercommunalités (AMF) ; Mme Constance Nebbula, vice-présidente de la région Pays de la Loire en charge du numérique et de l'intelligence artificielle et M. Alexandre Ventadour, conseiller territorial de Martinique, chargé du numérique et du développement économique, représentant l'association Régions de France ; ainsi que Mme Marlène Le Dieu De Ville, vice-présidente en charge du numérique à Intercommunalités de France, par ailleurs vice-présidente déléguée à l'économie numérique et aux systèmes d'information et à la culture de la communauté des communes de Lacq-Orthez. Elle s'exprimera également au nom de France urbaine.

Mesdames, messieurs, nous serons particulièrement attentifs aux points du texte qui vous paraissent poser difficulté, ainsi qu'à vos propositions concrètes pour en améliorer la mise en œuvre dans les collectivités.

M. Michel Sauvade, coprésident de la commission numérique nationale de l'Association des maires de France. Comme vous l'avez rappelé, les collectivités sont souvent en première ligne face à ces attaques, à telle enseigne que l'AMF y a consacré plusieurs ateliers dans le cadre de son congrès. Notre commission numérique se préoccupe régulièrement de ces sujets en partenariat avec l'Agence nationale de la sécurité des systèmes d'information (Anssi) et les services de l'État concernés.

Nous partageons l'ambition d'un renforcement de la cybersécurité pour les communes et les établissements publics de coopération intercommunale (EPCI), mais sommes très inquiets sur le contenu du projet de loi concernant les conditions dans lesquelles ces collectivités et EPCI devront mettre en œuvre les obligations. En effet, ces nouvelles obligations imposées par le projet de loi entraîneront des charges supplémentaires importantes pour les communes et les intercommunalités. J'ajoute qu'aucune étude d'impact n'a pu proposer jusqu'à aujourd'hui d'évaluation chiffrée de ces conséquences sur le plan financier et des ressources humaines.

Il existe simultanément une sorte d'injonction contradictoire de la part du gouvernement – du moins dans ses déclarations – et de la Cour des comptes, qui contestent l'augmentation des dépenses de fonctionnement du bloc communal. Quel que soit le caractère légitime de l'intention, cette injonction contradictoire pose problème.

Ensuite, compte tenu de la disparité des collectivités, nous regrettons que la loi ne puisse inscrire une progressivité qui permettrait justement de lisser ou d'atténuer les tensions attendues sur la filière des métiers cyber et les contraintes budgétaires que nous connaissons dans nos collectivités. Dans ce contexte, pour l'AMF, la transposition de la directive NIS 2 ne doit pas ignorer cette réalité et doit s'inscrire dans une logique de transition progressive et d'un accompagnement très marqué de l'État. Parallèlement, l'AMF demande que le périmètre des collectivités soumises à NIS 2 soit plus restreint, notamment pour les communautés d'agglomération et de communes.

Lors de la discussion au Sénat, des avancées ont été obtenues concernant justement le périmètre d'application pour les communautés d'agglomération, et l'AMF souhaite que, dans le cadre de la discussion à l'Assemblée nationale, le périmètre d'application pour les

communautés de communes soit également revu. Pour mémoire, l'AMF avait adressé un courrier au premier ministre le 7 mars dernier pour l'alerter justement sur cette situation des communautés d'agglomération et des communautés de communes.

Les propositions de l'AMF dans le cadre de ce projet de loi concernent seulement la directive NIS 2 et sont relatives aux mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. Le périmètre des entités essentielles retenu par le gouvernement pour les communes et les EPCI a évolué depuis la discussion au Sénat. Il résulte, nous semble-t-il, d'un choix du gouvernement qui peut être analysé comme une surtransposition de la directive.

Par ailleurs, l'AMF s'interroge sur le périmètre réel des communes concernées. Il n'est pas clair, notamment du fait des rapports étroits entre les communes et leurs EPCI, et de l'imbrication extrêmement variée des services informatiques et des mutualisations de personnel. Le référentiel de cybersécurité nous interroge également, puisqu'il dressera un tableau des prescriptions, réparties en une vingtaine d'objectifs applicables aux entités essentielles ou aux entités importantes, les obligations pour les entités essentielles étant plus contraignantes. Ces objectifs seront précisés ultérieurement dans un décret en Conseil d'État. En conséquence, le maire ou le président de l'EPCI sera *in fine* responsable de la sécurité numérique et du suivi de la conformité des systèmes d'information réglementés aux mesures édictées dans le référentiel de sécurité.

Quelles sont nos propositions ? L'AMF est soucieuse de la question de la cybersécurité et souhaite que l'application de cette directive soit un succès effectif. Toutefois, il faut que le législateur tienne compte de la réalité des moyens des communes et EPCI, afin que la mise en œuvre puisse être supportable financièrement, faisable techniquement et qu'elle soit progressive. Nous tenons donc vraiment à vous alerter sur la contradiction de ce texte avec les observations du gouvernement et de la Cour des comptes sur la maîtrise attendue de nos dépenses. De plus, il est difficile de concilier l'efficacité numérique et le maintien en l'état de nos systèmes d'information (SI).

Des consultations ont bien été conduites par l'Anssi, mais les préoccupations qui ont été exprimées par les associations d'élus n'ont pas reçu de réel écho à l'échelon politique, bien que l'AMF ait particulièrement insisté sur l'absence d'étude d'impact financier des nouvelles obligations, les nouvelles charges induites par les nouvelles obligations, l'absence de progressivité dans la mise en œuvre de la loi, le risque réel des tensions sur les métiers cyber et l'absence de visibilité sur un éventuel accompagnement de l'État.

L'adoption de la loi par le Sénat le 12 mars dernier a permis des avancées et l'AMF s'est félicitée de l'évolution concernant le périmètre de la loi pour les communautés d'agglomération. En revanche, toutes les communautés de communes sont restées assujetties au statut d'entités importantes, ce qui nous pose problème.

Les autres dispositions votées par le Sénat qu'il conviendrait de conserver concernent l'accompagnement de l'État. Le projet de loi prévoit que l'État élabore une stratégie nationale en matière de cybersécurité, comprenant notamment les modalités de soutien aux collectivités territoriales et leurs groupements. Concernant le règlement de sécurité, le décret en Conseil d'État qui déterminera les conditions d'élaboration de modifications éventuelles et de publication du référentiel s'appliquant aux entités essentielles et importantes devra être adapté à leur degré d'exposition aux risques, à leur taille, à la probabilité de survenance d'incidents et leur gravité, en prenant en compte également les conséquences économiques et sociales de

telles attaques. Ce règlement de sécurité devra également définir les modalités de concertation des représentants des entités concernées et des associations d'élus.

Concernant plus particulièrement la discussion à venir à l'Assemblée nationale, l'AMF demeure mobilisée. Nous souhaitons toujours que le périmètre d'application de la loi aux communautés de communes soit restreint. Je pense ici au non-assujettissement des communautés de communes inférieures à 30 000 habitants à NIS 2. En effet, nous sommes persuadés que la mise en œuvre sera pour le moins particulièrement difficile. Dans cette hypothèse, sur les 990 communautés de communes, seules 211 seraient assujetties au statut d'entité importante.

Parallèlement, il s'agit également de laisser le temps nécessaire à ces collectivités pour mettre en place de nouvelles règles de cybersécurité, lesquelles doivent être adaptées à leur réalité. Cette mesure a également pour objectif de ne pas créer une pression supplémentaire dans la mise en œuvre des règles de cybersécurité, alors que le marché est déjà sous tension.

Les communautés de communes entreront dans ce marché en même temps que de très nombreuses entreprises. Pour autant, il est utile d'assurer l'information et la formation des élus et des agents, ainsi que de promouvoir la diffusion des bonnes pratiques dans ces collectivités, comme dans les communes. À ce titre, je rappelle l'action de l'AMF pour sensibiliser les communes les plus petites, en partenariat avec les services de gendarmerie. Nous souhaitons que ces enjeux soient finalement inclus dans le projet de loi, en intégrant ce soutien, les programmes d'action de l'État et de ses opérateurs. L'AMF souhaite enfin une mise en œuvre progressive de la loi pour les communes et les EPCI assujetties à NIS 2 en métropole et dans les outre-mer.

Mme Marlène Le Dieu De Ville, vice-présidente en charge du numérique à Intercommunalités de France. À l'heure de la numérisation globalisée des services, du développement de la data, de l'intelligence artificielle (IA), des villes intelligentes et de la vidéosurveillance, la surface des attaques augmente de manière exponentielle pour tout le monde, y compris les collectivités. Ainsi, nous avons dénombré 187 attaques entre 2022 et 2023, mais ce chiffre tend à augmenter.

Nos associations Intercommunalités de France et France urbaine ont accueilli avec bienveillance la proposition de l'Anssi d'intégrer dans le dispositif NIS 2 l'ensemble des entités que nous représentons, aussi petites ou aussi grandes soient-elles. Nous saluons d'ailleurs l'écoute de l'Agence lors des diverses consultations. Nous positionnons l'intercommunalité comme l'espace de mutualisation et bassin de vie par excellence pour faire rempart.

En effet, Intercommunalités de France joue déjà un rôle majeur de cybersécurité en mutualisant les moyens humains, financiers et techniques pour protéger l'ensemble de ses communes membres face à un risque numérique grandissant. Avec la directive NIS 2, l'association deviendra un acteur clé pour accompagner les communes, notamment les plus petites d'entre elles, dans la mise en conformité avec les nouvelles obligations.

Grâce à cette approche collective et solidaire territoriale, les intercommunalités renforcent la résilience numérique des territoires, garantissant une meilleure protection contre les cyberattaques et une gestion plus efficace des ressources en cybersécurité. Depuis la réalisation de notre baromètre de maturité numérique des collectivités en 2023, nous avons pu

constater que sept intercommunalités sur dix ont au moins mis en œuvre des actions de sensibilisation et de formation auprès des agents et des élus. Aujourd'hui, une attaque peut concerner une petite commune de 200 habitants, mais entraîner des répercussions sur le système d'information de l'intercommunalité dont elle est membre. Il nous semble donc important d'intégrer tout le monde dans un dispositif, certes très lourd. Mais si nous le faisons de manière intelligente, cela fournira l'occasion de nous structurer dans ce domaine, puisque la cybersécurité et la cyberdéfense seront de toute façon notre quotidien.

Si nous accueillons avec bienveillance cette transposition à l'ensemble des collectivités que nous représentons, nous restons lucides. Nous sommes conscients des écueils qui pourraient empêcher l'effectivité de cette loi. Nous partageons effectivement les inquiétudes et les difficultés mentionnées par M. Sauvade. Dans un premier temps, nous exprimons un besoin de portage politique et de coordination ministérielle.

Nous avons pris connaissance des annonces récentes en termes de sensibilisation des 15 000 entités essentielles et importantes, dont les 1 500 collectivités qui devront s'enregistrer auprès de l'Anssi, mais nous avons peu de détails sur la manière dont cela se déroulera, ni sur l'accompagnement qui est attendu.

Par ailleurs, il est aussi parfois difficile pour les associations d'élus de traiter efficacement des sujets du numérique avec le gouvernement, car la coordination interministérielle est peu lisible. Par ailleurs, par l'intermédiaire des Interconnectés, nos deux associations d'élus ont lancé un groupe de travail dédié à l'élaboration de la phase réglementaire. Ce groupe miroir est composé de quinze collectivités allant de la communauté de communes à la métropole. Ce collectif a été réuni trois fois et a déjà pu analyser les impacts des objectifs de sécurité exprimés par la partie réglementaire.

Nous avons reçu les vingt objectifs de sécurité qui devront être traités et mis en œuvre. Ces objectifs de sécurité seront ensuite détaillés en sous-objectifs. Nous allons également échanger sur les leviers d'action et proposer des solutions à la future réglementation. Ce collectif a naturellement relevé des écueils importants, notamment en matière de compétences, de ressources humaines manquantes et d'obligations qui nous incombent d'après la réglementation, mais que nous serons dans l'incapacité de tenir. Les besoins concrets ont été regroupés dans un compte rendu qui sera remis à l'Anssi très prochainement. Après la validation de l'Anssi, nous serons en mesure de vous fournir ce document, si vous le souhaitez. Celui-ci explique l'ensemble de la démarche et ce que nous prévoyons de faire pour accompagner nos collectivités.

Je souhaite que nous puissions également parler de deux initiatives des Interconnectés qui sont étroitement associés à cette thématique : le groupe de travail « Petits territoires » et le projet « TIE Break » (Trajectoire d'indépendance européenne numérique). Ce dernier extraira l'ensemble des outils utilisés par nos collectivités (logiciels, outils de cyber, outils métiers), afin que l'Anssi les évalue et nous fournisse des préconisations.

En conclusion. rien ne sera possible sans un accompagnement technique et financier structuré. Un parcours cyber doté d'un audit précis a été proposé par France Relance, incluant un plan d'accompagnement pour améliorer la sécurité. Mais il n'a bénéficié qu'aux plus grosses entités, soit 78 communautés de communes sur 992. Il sera possible d'imaginer par la suite un « parcours NIS 2 », qui pourra être adapté en fonction des entités, au-delà d'un accompagnement purement financier. Enfin, un travail coordonné de toutes nos instances et structures sera nécessaire, quelle que soit leur nature.

M. le président Philippe Latombe. Nous sommes contraints par le temps lors de nos travaux. Pourriez-vous nous transmettre le document même s'il n'a pas été entièrement validé par l'Anssi ? Notre rapporteur pourrait ensuite échanger sur cette base avec l'Anssi. L'examen du texte devrait avoir lieu début juillet ou début septembre.

Mme Marlène Le Dieu De Ville. C'est entendu.

Mme Constance Nebbula, vice-présidente de la région Pays de la Loire en charge du numérique et de l'intelligence artificielle à Régions de France. Notre intervention s'effectuera à deux voix, puisque j'interviendrai en compagnie de M. Ventadour. Il s'agit pour nous de porter la parole des régions, qui sont extrêmement concernées par les directives aujourd'hui abordées, notamment parce que ces régions sont définies comme des entités essentielles. Notre objectif consiste à ce titre à vous indiquer les points bloquants, les risques techniques, financiers et organisationnels exprimés par les régions. Dans un premier temps, nous évoquerons le sujet cyber dans sa globalité, et notamment le périmètre qui pourrait être octroyé ou laissé aux régions. Dans un second temps, nous insisterons sur le lien avec l'Anssi, notamment sur le sujet des financements.

M. Alexandre Ventadour, conseiller territorial de Martinique, chargé du numérique et du développement économique à Régions de France. En préambule, je tiens à saluer la démarche de concertation engagée par votre commission. Je vous parle depuis la Martinique qui, il y a près de deux ans, a souffert d'une cyberattaque ayant mis à mal toute l'organisation de la collectivité territoriale.

Des préoccupations majeures se font jour de la part de l'ensemble des collectivités, dont les régions. La première concerne l'accompagnement de ces collectivités. Les régions sont ainsi désignées comme des entités essentielles. Le texte prévoit un délai de trois ans pour se mettre en conformité, mais en ne précisant pas assez les moyens qui seront associés, qu'il s'agisse des moyens humains ou financiers qui doivent être adaptés, notamment s'agissant des CSIRT (*Computer Security Incident Response Team*). Ce délai de trois ans risque donc de ne pas suffire, tant les obligations prévues sont lourdes (cartographie, audits, plans de sécurisation, suivi des incidences et gouvernance). Certaines régions font face à des réalités complexes.

D'autres territoires, comme la Martinique et la Réunion, ont également souffert de sévères attaques. Plus largement, les outre-mer ne disposent pas forcément des ressources en interne. Lorsque la Martinique a subi cette cyberattaque, je me souviens avec émotion avoir vu débarquer une équipe d'une douzaine de techniciens – notamment de l'Anssi – pour venir à notre secours, mais ils n'ont pas pu rester pendant toute la durée du sinistre. Nous avons donc été contraints de fonctionner ensuite à distance. Cet exemple montre bien que les territoires éloignés ne sont pas forcément armés pour résister à de telles attaques.

Le projet de loi introduit dans son article 5 *bis* la notion de stratégie nationale de cybersécurité, pilotée par le premier ministre. Nous nous en félicitons et demandons que cette stratégie prévoie explicitement les modalités de soutien opérationnel et budgétaire aux collectivités, par exemple en lien avec les objectifs et les financements de France 2030.

Deuxièmement, aucune étude d'impact n'a été véritablement menée sur les coûts engendrés pour les collectivités. La ministre en charge du numérique a reconnu en audition que les collectivités devraient consacrer jusqu'à 10 % de leur budget informatique à la cybersécurité. Pour certaines régions, notamment les plus importantes, cela représenterait

plusieurs millions d'euros par an, sans compter les audits et formations préalables ou le remplacement des infrastructures obsolètes. En outre, NIS 2 ne concerne pas uniquement les opérateurs publics et les agents, mais également les partenaires et prestataires avec lesquels nous allons devoir travailler, qui devront être labellisés. Or, dans certaines régions, ces partenaires n'ont pas forcément les moyens de monter en puissance ; il sera nécessaire de les accompagner. Nous demandons donc que l'État commande une étude de coût exhaustive, afin de financer réellement la montée en puissance exigée par NIS 2.

Troisièmement, il convient d'évoquer le périmètre d'action. Lors de nos discussions au sein de Régions de France, a été relevé un point d'attention concernant les lycées. En effet, ces établissements relèvent des régions. Le projet de loi ne précise pas si les infrastructures informatiques des lycées rentrent dans le périmètre de responsabilité des régions au titre de la directive. Or il peut s'agir parfois de dizaines de milliers de postes informatiques, dont les niveaux de sécurisation sont très hétérogènes. En conséquence, nous demandons une clarification explicite dans les décrets d'application, afin d'éviter un vide juridique ou une responsabilité mal encadrée.

Les régions ne contestent pas le projet de loi, qu'elles appellent au contraire de leurs vœux. Pour autant, sa mise en œuvre doit être pragmatique, équitable et accompagnée. Nous attendons que l'État, aux côtés des régions, mais plus largement des collectivités, joue également un rôle d'accompagnateur et de financeur.

Mme Constance Nebbula. J'insisterai pour ma part sur la relation avec l'Anssi telle qu'elle est envisagée dans le projet. Je pense notamment à la création des organismes relais agréés par l'Anssi prévus à l'article 24 du projet de loi. Il est ainsi indiqué que l'Anssi peut agréer des organismes publics ou privés, en tant que relais dans la prévention et la gestion des risques cyber.

Il apparaît intéressant de considérer que les CSIRT et les dynamiques autour des campus cyber des régions sont naturellement pressentis pour assurer ce rôle d'organisme-relais agréé par l'Anssi dans les territoires. Ces éléments conduisent à soulever un certain nombre de questions. Quels seront les moyens financiers alloués par l'État aux régions pour leur permettre de faire vivre ces structures ? Serait-il possible de développer une forme de labellisation NIS 2 pour attester de la conformité des entités qui sont concernées par le champ d'application de la loi « Résilience et cybersécurité », notamment pour permettre à ces entités de justifier plus simplement de leur conformité à la directive en cas de contrôle ?

Il s'agirait donc de faciliter la conformité des entités régulées, mais pour permettre de développer une offre complémentaire pour les CSIRT. Cette valeur ajoutée offrirait la possibilité d'équilibrer un modèle financier qui n'est pas trouvé aujourd'hui. S'agissant de cette question de labellisation, il serait opportun que la ministre du numérique confie à l'Anssi la mission de définir un label de conformité, afin que les entités puissent s'en prévaloir. L'Anssi prendrait donc le contrôle de l'agrément et aurait accès à un label valorisant l'engagement des CSIRT, notamment en région, pour pérenniser leurs actions.

Nous demandons également la prolongation du financement. Régions de France a d'ailleurs adressé un courrier au premier ministre il y a quelques semaines à ce sujet. Bien entendu, les régions ne sont pas surprises de l'arrêt du financement. En revanche, une dynamique cyber nationale avait été amorcée avec le lancement des CSIRT, qui va malheureusement s'interrompre, laissant le relais aux régions. Cet aspect pose nécessairement question. Pour rappel, l'Anssi avait consacré 1 million d'euros à cette initiative sur une

période de trois ans, qui arrive aujourd'hui à son terme. Nous opérons donc en mode « débrouille » pour continuer à faire vivre ces CSIRT, en l'absence du soutien de l'État.

Au-delà du financement, des nouveaux acteurs sont apparus dans la chaîne, notamment le 17Cyber, plateforme portée par Cybermalveillance.gouv.fr. De leur côté, les CSIRT sont organisés autour de centres d'appels traités par des opérateurs issus des partenaires et prestataires connus, labellisés, sécurisés, en région et en proximité. Il s'agit donc de trouver le bon partenariat entre ces différents outils, ce qui n'est pas forcément évident, compte tenu de la différence de points de vue entre Cybermalveillance.gouv.fr et les régions.

Régions de France demande que l'État participe au financement et à la pérennité des CSIRT par l'intermédiaire de l'Anssi et clarifie les rôles de Cybermalveillance.gouv.fr et de l'Anssi, au-delà de la simple signature de partenariats, lesquels sont très différents d'une région à l'autre. À ce titre, nous déplorons un certain manque d'uniformité et de vision nationale.

En conclusion, les régions sont vraiment vigilantes concernant la préparation des décrets d'application, notamment le décret relatif à l'élaboration du référentiel d'exigences techniques et opérationnelles. Par ailleurs, les régions n'ont pas attendu les discussions du moment pour anticiper et travailler sur le risque cyber. Néanmoins, nous souhaiterions être accompagnés, soutenus, dans le cadre d'une dynamique nationale.

M. Éric Bothorel, rapporteur général. Nous sommes tous convaincus que les moyens financiers qu'il sera nécessaire de réunir, fussent-ils soutenus par l'État, ne sont pas commandés par NIS 2, mais par l'état de la menace et de l'activité cybercriminelle. De fait, l'Anssi a dû traiter 218 incidents cyber concernant les collectivités, dont 144 ayant trait aux communes, soit une moyenne de dix-huit par mois. Nous portons donc une responsabilité collective, afin de mettre en œuvre des éléments nous permettant de faire face à cette activité cybercriminelle. Pour reprendre les mots de Vincent Strubel, nous avons tous découvert qu'il n'est pas nécessaire d'être une cible pour être une victime. Les collectivités continuent de l'apprendre à leurs dépens. Il conviendra évidemment, au travers de ce texte, qui s'inscrit dans une doctrine européenne, de trouver les organisations qui nous permettent d'être plus résistants, plus résilients et plus efficaces.

Ma collègue Anne Le Hénanff est rapporteure de la partie du projet de loi relative à NIS 2. Étant retenue en circonscription, elle m'a transmis ses questions, que je m'apprête à vous poser, tout en partageant ses préoccupations. Quel est votre avis sur les ajouts et modifications apportés par le Sénat concernant les collectivités territoriales ? Jugez-vous le seuil des 30 000 habitants pertinent et adapté ? À défaut, quel seuil privilégieriez-vous ? Pour ma part, je suis surpris que le Sénat n'ait pas traité de manière identique les communautés d'agglomérations et les communautés de communes.

Quel est votre avis sur les critères retenus par la Belgique pour déterminer si une collectivité était assujettie ou non aux dispositions de la directive NIS 2 ? Avez-vous évoqué avec l'Anssi le cas des communes dites touristiques dont la population permanente est inférieure à 30 000 habitants mais pouvant aisément dépasser ce seuil en période estivale ? Compte tenu des services publics dont elles disposent, pensez-vous qu'elles devraient être assujetties à NIS 2 ? Enfin, quel est le retour des collectivités concernant la solution des CSIRT régionaux ? Les sollicitent-elles ? De quelle manière ? Quelle est en pratique l'aide

apportée ? Est-elle optimale ? D'après vous, les CSIRT doivent-ils jouer un rôle dans la mise en œuvre de NIS 2 ?

Madame Nebbula, je ne suis pas opposé à l'idée d'un modèle différent pour les CSIRT. Le président de ma région est ainsi très attaché à l'expérimentation et à la différenciation. Le fait que les campus cyber et les CSIRT reposent sur les modèles différents ne fait pas obstacle à une bonne coordination entre eux pour une meilleure efficacité dans un dispositif plus global.

Mme Constance Nebbula. Tout d'abord, je vous remercie de prendre le temps de conduire cette concertation. Nous avions d'ailleurs eu l'occasion de l'indiquer au Sénat au début du mois de février, tant ces occasions sont rares. Nous profitons de NIS 2 pour évoquer ces sujets, pour parler de stratégie, de politique cyber, mais aussi des financements, des moyens, de l'organisation. C'est peut-être un peu tardif ; néanmoins, mieux vaut tard que jamais.

Lors de la discussion au Sénat, Régions de France a rappelé son attachement à une vraie stratégie de l'État en matière de cybersécurité. La nouvelle rédaction du projet de loi comprend de fait « l'élaboration » par le premier ministre d'une stratégie nationale en matière de cybersécurité, inscrite dans le nouvel article 5 *bis*, qui détaille les modalités de soutien aux collectivités territoriales et à leurs groupements. Il y a là deux signaux très intéressants, qu'il faut pérenniser : une véritable ambition politique stratégique en matière de cybersécurité ; et la définition des modalités de soutien aux collectivités territoriales et à leurs groupements. Nous considérons que ces éléments vont dans le bon sens et qu'ils doivent être pérennisés.

La deuxième question concernant Régions de France porte plus sur les CSIRT. Lorsque nous indiquons que chacun dispose de modèles différents, il ne s'agit pas d'une critique. Simplement, les solutions à nous apporter ne sont peut-être pas identiques pour tout le monde. Par exemple, il n'existe pas de CSIRT en Martinique ; certaines régions possèdent des campus cyber, d'autres non ; ailleurs, les CSIRT sont parfois intégrés à des campus cyber. À l'occasion de la concertation conduite avec nos collègues, nous avons été unanimes pour témoigner de notre volonté de bénéficier d'un accompagnement, au-delà d'un soutien financier. Nous sommes tous élus locaux et savons bien que le contexte budgétaire est compliqué.

Néanmoins, j'insiste pour signifier que nous évoluons tous aujourd'hui dans un mode « débrouille ». L'Anssi nous a aidés à effectuer l'amorçage, mais encore faut-il désormais trouver le modèle, les ressources humaines et les partenaires. À titre d'exemple, dans les Pays de la Loire, nous n'avions pas jusqu'à présent de structure juridique.

Il est donc nécessaire d'élaborer une vision nationale sur la manière dont les collectivités travailleront avec l'Anssi, mais également la répartition des rôles entre l'Agence, Cybermalveillance.gouv.fr, la gendarmerie et les différents dispositifs. Les très petites entreprises (TPE) et les petites et moyennes entreprises (PME) font aujourd'hui face à un flot très important de possibilités.

Soit chaque région communique bien sur son outil régional, mais la communication nationale n'est pas optimale ; soit la situation est inverse. Des choix doivent donc être opérés. De notre côté, nous considérons que ce qui est porté localement a plus d'impact que ce qui est porté sur le plan national. Mais les deux démarches doivent se dérouler en bonne entente, préalablement à la signature d'un partenariat.

M. Alexandre Ventadour. Il est exact que la Martinique n’a pas de CSIRT. Au moment où il était question de les mettre en place, nous avons été frappés par la très grande cyberattaque dont je parlais précédemment, laquelle a laissé des traces, encore visibles aujourd’hui. La mise en place n’a pas eu lieu, faute de visibilité sur le financement après « l’expérimentation » de trois ans. Comme de nombreuses collectivités, les territoires ultramarins ont connu des actions initiées sur le plan national, qui étaient ensuite basculées sur le financement propre des régions.

Nous ne disposons pas de CSIRT, mais nous tâchons de répondre aux incidents. Quoi qu’il en soit, nous nous efforçons de revenir dans cette initiative importante, qui nous met en lien avec l’ensemble du territoire. Les CSIRT doivent à la fois coopérer entre elles, mais aussi avec l’entité étatique. Il ne s’agit pas uniquement de protéger nos collectivités, mais également de permettre aux PME et TPE avec lesquelles nous travaillons, notamment sur ces aspects informatiques, numériques et de cybersécurité, de pouvoir monter en compétence.

C’est la raison pour laquelle nous en appelons à une forme de labellisation qui pourra en outre contribuer à l’établissement d’un *business model*, en étant conscient que l’argent public se fait rare actuellement. Nous savons pertinemment qu’il n’est pas possible de tout régler avec un financement national. C’est la raison pour laquelle nous proposons des solutions alternatives – car dans les domaines régaliens comme la sécurité ou la santé, les activités ne peuvent pas dégager de profits – si nous ne voulons pas concurrencer les acteurs privés de nos territoires, qui ne profitent pas de leur côté de l’argent public.

En conclusion, une forme de modèle hybride de financement sur les CSIRT régionaux serait extrêmement intéressante et extrêmement efficace, notamment pour la proximité de l’action.

Mme Marlène Le Dieu De Ville. Le seuil de 30 000 habitants constitue un critère important dans la proposition initiale de l’Anssi. Comme cela a été relevé par la commission supérieure du numérique et des postes, ce critère n’est sans doute pas le plus pertinent. Initialement, lorsque cette proposition d’intégrer les intercommunalités dans NIS 2 a été formulée, il était également prévu que les communautés de communes de plus de 30 000 habitants, soient considérées comme entités essentielles, les autres étant des entités importantes.

L’Anssi n’avait pas conscience de l’existence de communautés de communes de 80 000 habitants ; elle pensait qu’au-delà de 30 000 habitants, le format de la communauté d’agglomération s’imposait. Nous avons donc expliqué que cela n’était pas le cas, ce qui a permis de rectifier le tir. Nous avons également souligné qu’entre une communauté de communes de 5 000 habitants et une autre de 80 000 habitants, les disparités de moyens sont telles que les services informatiques sont structurés différemment. Ces disparités ont éclaté au grand jour lors des plans France Relance et des parcours cyber, puisque seules les plus importantes collectivités ont été accompagnées, ce qui est à la fois quelque peu aberrant, mais également logique.

Quels peuvent être les autres critères ? La commission supérieure du numérique et des postes avait proposé que l’Anssi décide en fonction des compétences critiques, voire très critiques, que chacune collectivité peut exercer. Par exemple, une ville balnéaire qui voit sa population passer de 10 000 habitants à 100 000 habitants l’été pourrait être intégrée à juste titre dans le dispositif.

En conséquence, nous avons également relevé de notre côté quelques incohérences. Le Sénat n'a pas imposé aux communes de transférer les compétences pour le secteur dit critique de l'eau et de l'assainissement, faisant naître des situations complexes. Certaines communautés de communes intégreront ainsi l'eau et l'assainissement dans leur périmètre, mais cela ne sera pas le cas pour toutes. Nous nous posons des questions, puisque les communes de moins de 30 000 habitants ne sont pas soumises à NIS 2.

En résumé, le critère du nombre d'habitants n'était pas le plus pertinent, mais il faut désormais s'en accommoder. En outre, des amendements ont pu voir le jour. Je salue à ce titre celui qui permet aux communautés d'agglomération qui n'ont pas de villes de plus de 30 000 habitants de sortir du périmètre « entité essentielle ».

S'agissant de la coordination régionale, nos groupes de travail ont souligné la nécessité d'un accompagnement plus proche et plus local. Nous avons besoin de savoir à qui nous nous adressons et qui peut nous accompagner. En Nouvelle-Aquitaine, le CSIRT est imbriqué dans le campus cyber ; les relations sont bonnes. Mon intercommunalité fait partie du campus cyber et le travail est intéressant. Cependant, nous aimerions aller plus loin, à travers une généralisation au niveau national.

Par ailleurs, nous souhaitons que l'Anssi assure une présence plus active au niveau régional, pour nous accompagner dans toutes nos démarches.

M. Michel Sauvade. Nos échanges témoignent de la vision partagée des associations d'élus. À l'AMF, la commission numérique est présidée par deux élus, l'un étant vice-président d'un département et l'autre vice-président d'un conseil régional. Il existe donc naturellement une coordination sur cet ensemble. La table ronde de ce jour montre également l'absence de portage politique. En tant que parlementaires et élus locaux, nous avons une responsabilité dans l'absence de ce portage.

Lorsque nous échangeons avec les directeurs des systèmes d'information (DSI) ou les responsables sécurité des systèmes d'information (RSSI), ils nous reprochent de les placer en première ligne sans qu'ils ne disposent pour autant de visibilité, ni de soutien. À l'AMF, nous avons en effet organisé une rencontre avec des DSI, dont les conclusions ont été assez perturbantes. Nous parlons aujourd'hui de la transcription de la directive NIS 2, mais plus globalement, les communes sont aujourd'hui confrontées à un problème de ressources humaines, pour pouvoir trouver des spécialistes en mesure de gérer nos réseaux et d'administrer nos serveurs.

Les amendements sénatoriaux sont intéressants, mais le travail doit être poursuivi. Je partage également l'interrogation concernant ce seuil des 30 000 habitants. Dans un souci de lisibilité, ce seuil pourrait emporter une cohérence globale dans le dispositif.

Ensuite, dans les communes touristiques, des blocages peuvent intervenir, mais il ne s'agit pas de cyberattaques. Ce problème du blocage est ainsi lié à l'insuffisance des infrastructures. Nous sommes sollicités par les communes, notamment en termes de couverture numérique. Lorsque des phénomènes de saturation surviennent, le système se bloque, non pas par malveillance, mais en raison de l'inadaptation des moyens.

D'une manière plus générale, pour les législateurs que vous êtes, l'enjeu consistera dans les semaines à venir à faire vivre et évoluer un texte, afin qu'il s'adapte au plus près du terrain, dans l'échelle, la temporalité, mais aussi dans l'anticipation en matière de

cybersécurité. Dans le cadre de NIS 2, il ne s'agit pas d'agir en curatif, mais bien d'être capable d'anticiper une attaque qui, de toute façon, se produira à un moment ou un autre.

M. Thomas Gassilloud (EPR). En tant qu'ancien « jeune élu », je confirme que nous partons effectivement de loin en matière cyber. Il n'en demeure pas moins que le numérique est capital dans nos collectivités et que nous devons collectivement renforcer notre cybersécurité.

Je souhaite également revenir sur la question du seuil. Je partage l'idée que le critère du nombre d'habitants n'est pas forcément le plus adéquat, compte tenu des modes de gestion et des compétences très différentes, mais il s'agit peut-être du moins mauvais. Je n'ai pas encore suffisamment étudié le texte pour me positionner sur la pertinence du seuil à 30 000 habitants, mais il m'apparaît nécessaire de faire confiance aux élus pour déterminer l'approche en matière de cyber dans leur collectivité, dans une logique de subsidiarité et de libre administration des collectivités territoriales.

Lorsque j'étais élu local, j'ai ainsi constaté que les directives imposées par le niveau national coûtaient cher et n'étaient pas toujours appropriées. Au-delà, nous devons tous être vigilants quant au maillage des collectivités : si l'on en impose toujours plus aux collectivités, nous risquons de fragiliser l'existence de collectivités de plus petite taille. Or nous sommes pourtant toujours contents de trouver nos maires de proximité lorsqu'il s'agit de traiter des situations de crise, telles une crise sanitaire ou une crise cyber. Par-delà la transposition de NIS 2, ce texte peut nous permettre collectivement de développer la culture du risque et la culture de défense dans nos collectivités, dans une logique d'efficacité.

Comment la déclinaison de NIS 2 peut-elle constituer l'occasion d'une approche plus globale pour prévenir les risques au sens large dans nos collectivités, en lien avec les dispositifs existants, les correspondants défense, la gendarmerie nationale, les plans communaux de sauvegarde, les réserves communales de sécurité civile ? Par ailleurs, je suppose que les collectivités sont également soumises à certaines dispositions de la directive REC puisqu'elles gèrent des services d'énergie, d'eau et de transport. Quels sont les impacts de cette directive pour les collectivités territoriales ?

M. Arnaud Saint-Martin (LFI-NFP). Je remercie les intervenants pour ces éléments de restitution, qui montrent à quel point il est nécessaire d'investir massivement pour assurer la sécurisation des infrastructures et systèmes de nos collectivités locales. Lorsque j'étais élu municipal et communautaire de Melun, j'ai suivi de très près une cyberattaque qui a déstabilisé brutalement et durablement les services informatiques du conseil départemental de la Seine-et-Marne. Celle-ci fut le ferment d'une prise de conscience essentielle.

Je souhaite évoquer la consolidation d'une culture partagée des risques cyber. Le projet France Relance, lancé en 2021, consistait à investir 250 millions d'euros pour rapprocher le numérique du quotidien des Français. Dans ce cadre, 4 000 conseillers numériques ont été recrutés sous la forme de contrats aidés sur tout le territoire, formés et financés par l'État. Or ce projet doit s'arrêter en 2027, alors même que l'ensemble des objectifs n'ont pas été atteints. Les premiers contrats des conseillers se sont arrêtés en 2023 ; la seconde vague de fin de contrats interviendra en 2025 et la troisième en 2027. Par ailleurs, 13 millions de Français sont éloignés du numérique. La situation ne s'est pas améliorée, voire s'est dégradée, avec l'explosion de l'intelligence artificielle et l'augmentation des menaces cyber.

Face à ce constat, il est évident que les conseillers numériques sont essentiels dans les collectivités. En complément de France Services, ils accompagnent les usagers les plus vulnérables et les plus éloignés du numérique dans leurs démarches en ligne. Un travail immense reste à accomplir à travers une politique massive d'éducation d'une grande partie de la population pour faire face aux diverses menaces cyber qui peuvent aussi toucher les particuliers.

Il est donc urgent de construire une politique nationale stable de la médiation numérique. Le plan France Relance, mis en place depuis 2021, a souffert d'un cruel manque de stabilité – contrats aidés, contrats courts, sous-traitance – et d'un manque de planification. Les conseillers numériques recrutés restent en moyenne moins d'un an et demi en poste, dont six mois qui servent à pleinement les former. Il est pourtant nécessaire que le rôle des conseillers numériques soit étendu en lien avec ce projet de loi, pour faire face aux menaces, accompagner les usagers les plus vulnérables. De tels chantiers justifieraient une prolongation du rôle de ces conseillers et le réarmement d'une politique publique de la médiation numérique interministérielle.

Pour assurer la résilience numérique et l'adaptation de l'ensemble de la population, quel dispositif vous semble le plus utile à soutenir sur un plan budgétaire ? Que préconisez-vous pour assurer une politique d'éducation populaire aux enjeux de cybersécurité ? Pensez-vous qu'il soit nécessaire de pérenniser les emplois de conseillers numériques dans le cadre de ce projet de loi ?

Mme Geneviève Darrieussecq (Dem). Je partage également l'idée que notre société a besoin de prendre en compte ces risques cyber. Nous travaillons longuement sur ces sujets dans le cadre de la commission de la défense et constatons que nous sommes très vulnérables, à tous les niveaux. Les grandes entreprises réussissent à organiser leur défense, mais les PME et TPE éprouvent plus de difficultés. Le même parallèle peut être établi entre grandes et petites collectivités, qui sont par ailleurs liées entre elles par des liens numériques, qui constituent autant de fragilités potentielles.

En conséquence, nous devons tous être protégés. Quelle est selon vous la bonne échelle pour la mise en place de moyens organisationnels sur le terrain ? Faut-il privilégier un grand campus régional, un échelon départemental ? Enfin, il ne faut pas distinguer les besoins des entreprises et ceux des collectivités. Nous sommes embarqués dans le même bateau et souvent interconnectés.

Mme Laetitia Saint-Paul (HOR). Lorsque la commission des affaires étrangères a auditionné le directeur de l'Anssi, il a indiqué que les hackers ou les rançongiciels mettent en œuvre des ciblages très intelligents. Plutôt que d'attaquer frontalement, ils passent par les portes dérobées ; par les sous-traitants pour les entreprises, par les entités secondaires, pour les collectivités. Dès lors, je rejoins également l'interrogation de mes collègues concernant le seuil des 30 000 habitants, puisque ces hackers emploient des méthodes de contournement.

Ensuite, nous sommes très attachés à nos départements et régions d'outre-mer. J'ai acquis la certitude que ces outre-mer représentent la cible principale des stratégies hybrides qui s'attaquent à notre pays. Nous avons pu le constater lors des manœuvres d'ingérence étrangère de l'Azerbaïdjan envers la Nouvelle-Calédonie. Les outre-mer constituent également une cible dans le cadre de la lutte pour les espaces communs à l'échelle mondiale – notamment l'espace maritime. Leur éloignement des structures de soutien métropolitaines les

rend d'autant plus vulnérables. Dès lors, ce projet de loi peut leur permettre d'améliorer leur cyberdéfense, qu'elle soit civile ou militaire. Je souhaite donc vous interroger à ce sujet.

Enfin, j'ai été interpellé par la remarque de Mme Le Dieu De Ville s'agissant des problèmes de communication interministérielle. J'espérais pour ma part que sous l'égide du secrétariat de la défense et de la sécurité nationale (SGDSN), l'interministériel fonctionnerait. Pouvez-vous détailler à quel point les dysfonctionnements interministériels que vous avez mentionnés sont problématiques ?

Mme Marlène Le Dieu De Ville. Pour ma part, je fais partie d'un groupe de travail sur la résilience des territoires, en lien avec les entreprises de vidéoprotection et le SGDSN, mais ce dernier n'est pas notre interlocuteur principal à l'heure actuelle. Dès lors, il pourrait être intéressant de travailler avec cette structure de manière plus régulière. Nous regrettons à ce titre l'absence d'un interlocuteur unique, tant il est vrai que sur ces sujets, nous devons nous adresser à des ministères ou des secrétariats d'État différents en fonction des sujets. De plus, les actions des uns et des autres ne semblent pas forcément toujours coordonnées ; elles peuvent même sembler parfois concurrentes. Je pense notamment à la confusion engendrée par l'existence simultanée des conseillers numériques France Services et des conseillers France Services. Il m'a ainsi fallu du temps pour comprendre qu'il s'agissait d'acteurs différents. En résumé, nous sommes preneurs d'un interlocuteur unique. Si nous ne pouvons pas disposer d'un ministre dédié, il pourrait être intéressant de travailler avec le SGDSN.

Ensuite, les intercommunalités se proposent d'être un espace de mutualisation en fonction des besoins des communes qui les composent. Il nous avait été proposé de prendre une compétence cybersécurité, mais nous ne le souhaitons pas. Nous pouvons en revanche mutualiser des formations et des ressources humaines. Les plans communaux et intercommunaux de sauvegarde constituent ou constitueront des outils qui devraient être améliorés.

La culture partagée et les conseillers numériques France Services représentent une préoccupation portée par Intercommunalités de France et les Interconnectés depuis un certain temps. Nous avons appelé à la pérennisation des conseillers numériques France Services, qui constituent la cheville ouvrière de la transition numérique et de la cybersécurité. Dans mon territoire, la collectivité de communes Lacq-Orthez, nous avons la chance de disposer de six médiateurs numériques. Ils sont salariés par nos soins et ont pour objectif d'accompagner tous les publics, qu'il s'agisse de nos agents, mais également de la population, dans tous les domaines et sur tous les enjeux du numérique, dont la cybersécurité.

Forts de cette expérience, nous nous battons afin que ces conseillers soient *a minima* pérennisés. Hier, nous avons discuté avec les membres de la commission des finances de l'Assemblée nationale pour étudier précisément le financement de cette pérennisation, dans un contexte budgétaire difficile. En effet, ils sont indispensables à cette transition numérique et il importe de ne laisser personne de côté, d'autant plus que les agences de proximité ont été fermées. Selon une étude, l'État enregistrerait une perte de 1,6 milliard d'euros si les personnes n'étaient pas accompagnées d'une manière ou d'une autre.

Quel est le bon échelon ? Intercommunalités de France souhaite travailler sur cette directive NIS 2 et que ses membres y soient intégrés, quitte à établir quelques aménagements. Je partage les propos de Mme Saint-Paul concernant le mode opératoire à partir de portes dérobées. À titre d'exemple, une école de commerce a été attaquée, puis le problème s'est répandu aux autres écoles appartenant au même réseau, s'est diffusé à la chambre de

commerce et d'industrie dont dépendait l'école et a finalement impacté fortement un aéroport. Il est possible d'imaginer qu'une petite commune serve de point d'entrée pour diffuser une attaque vers la communauté de communes, l'agglomération, la métropole et éventuellement un hôpital.

Les échelons locaux sont très importants, mais il est surtout essentiel de se concentrer sur la coordination. Par ailleurs, les intercommunalités et les régions partagent la compétence en matière de développement économique. Il est donc important de veiller à maintenir une relation étroite avec cet échelon régional. J'ajoute que l'échelon départemental n'est pas en reste, puisque nous travaillons avec des structures comme les opérateurs publics de services numériques (OPSN).

En résumé, l'enjeu ne porte pas tant sur l'échelon pertinent, mais sur la manière dont nous arrivons à travailler ensemble, de manière coordonnée, les uns avec les autres, en évitant les effets de concurrence.

Mme Constance Nebbula. Monsieur Gassilloud, vous avez évoqué le principe de subsidiarité et la nécessité de laisser la main libre aux collectivités. Je salue cette attention, mais souligne que la cybersécurité demeure malgré tout un sujet régalien. Il ne faudrait pas que l'État profite de la discussion en cours pour se désengager de sa mission. Je considère également qu'il ne revient pas aux collectivités locales de s'occuper de la cybersécurité des autres collectivités. De notre côté, nous avons opéré le choix d'accompagner notre cible préférentielle, c'est-à-dire le monde économique au sens très large. De fait, chaque strate de collectivité dispose de son public et doit intégrer la cybersécurité dans le cadre de ses compétences. En revanche, les domaines régaliens, la coordination, la stratégie, le portage politique et l'interlocuteur unique relèvent bien de l'État. Au-delà, je partage moi aussi l'idée d'un nécessaire développement d'une culture du risque du cyber et du numérique.

Aujourd'hui, les collectivités locales payent les conseillers numériques, faute d'avoir pu trouver des solutions pérennes au niveau national. Ici aussi, nous nous débrouillons, face à l'absence de pérennité du dispositif. Chaque conseiller numérique intègre ainsi la dimension cyber dans son accompagnement.

Vous avez ensuite évoqué les moyens organisationnels. Nos collectivités sont confrontées à un problème de compétence et de recrutement. Les métiers de RSSI sont nouveaux pour les collectivités et les experts cyber ne sont pas incités à travailler dans le public, puisqu'ils peuvent être bien mieux rémunérés dans le privé. En outre, les assurances rechignent à assurer les risques cyber. Pourquoi voudraient-elles assurer un risque qui se matérialisera de toute manière ? Par exemple, la métropole d'Angers n'est plus couverte dans certains domaines. Nous avons réouvert des marchés, mais aucun assureur n'a voulu y répondre. Comment agir dans de tels cas ? Faut-il obliger les assureurs ?

Encore une fois, je considère que l'échelon régional est le plus intéressant pour la cible économique que constituent les TPE, les PME et les petites et moyennes entreprises (PMI). J'aimerais qu'un interlocuteur unique existe, mais pour y parvenir, il faudrait des moyens, une ambition, une coordination nationale. Malheureusement, je pense qu'il est trop tard ; les actions ont été trop éparpillées.

Enfin, il me semble que le SGDSN s'occupe plutôt des infrastructures. Je constate également que nos liens avec ce dernier sont assez lâches. À l'heure actuelle, les relations interministérielles fonctionnent très mal en matière de cyber. Dans ce domaine, il n'existe pas

d’interlocuteur unique et nous ne savons pas vers qui nous diriger. De la même manière, nous rêverions d’avoir un interlocuteur politique ou administratif unique, mais ceux-ci n’existent pas.

M. Alexandre Ventadour. Ce sujet est effectivement éminemment politique, particulièrement aujourd’hui alors que les problèmes de souveraineté et de géopolitique s’intensifient. Il ne s’agit pas seulement d’attaques crapuleuses, mais bien souvent de tentatives de déstabilisation. Je partage les propos de Mme Nebbula : en matière cyber, le millefeuille administratif a été reproduit, quand nous aurions dû agir en bloc. Lorsque le 17Cyber a été créé, j’avais espoir qu’il constituerait une réponse lisible et unique, mais nous n’en prenons pas véritablement le chemin.

Ensuite, je remercie Mme Saint-Paul pour ses propos concernant les outre-mer. Au-delà de la problématique de l’éloignement de la métropole, les outre-mer constituent des territoires relativement riches, dans des zones souvent relativement pauvres. Elles constituent donc des cibles de choix pour les pirates cybernétiques, comme en témoignent les attaques subies par la Martinique, la Guadeloupe, la Guyane ou La Réunion.

Nous sommes sous-dotés en ressources humaines spécialisées. Mme Nebbula a évoqué les difficultés en matière de recrutement en métropole ; celles-ci sont décuplées dans les territoires ultramarins. À titre d’exemple, il nous a fallu un an et demi pour recruter le RSSI de la collectivité de Martinique. En outre, nos infrastructures sont vieillissantes, éclatées et nous sommes soumis à une forte dépendance vis-à-vis des prestataires. Malgré nos efforts, il est difficile d’en trouver localement et nous devons faire appel à des prestataires situés à plus de 6 000 kilomètres, ce qui contribue à rallonger les délais d’intervention. Néanmoins, nous avons essayé de trouver des solutions et de nous organiser, notamment sur la partie atlantique des régions ultrapériphériques des départements et régions d’outre-mer ; mais les moyens demeurent insuffisants.

En conséquence, nous préconisons d’inscrire l’outre-mer en « particularité » dans les projections et les propositions pour résorber l’éloignement non seulement kilométrique, mais aussi en termes d’accès à la performance, à la compétence et au financement nécessaire. Nous prônons donc une compensation pour ces territoires, qui sont plus attaqués que les autres.

De son côté, la collectivité de Martinique s’efforcera de continuer à éduquer et sensibiliser les populations à l’utilisation éthique, sécurisée de l’intelligence artificielle. Mais plus les usages de la chose digitale se développent, plus il est nécessaire d’apporter des solutions de sécurité appropriées.

M. Michel Sauvade. Je remercie les députés pour leurs questions, qui témoignent de l’intérêt pour les collectivités locales.

Monsieur Gassilloud, vous avez à juste titre souligné le nécessaire développement de cette culture du risque. Monsieur Saint-Martin, vous avez quant à vous relevé l’importance du portage politique, mais je dois avouer que nos expériences en la matière n’ont pas été forcément toutes concluantes. Je me souviens par exemple d’un chef de cabinet intervenant par visioconférence pour expliquer aux associations d’élus que les conseillers numériques, qui devaient être initialement embarqués à hauteur de 4 000, le seraient finalement à hauteur de seulement 1 500, suscitant par là-même l’incompréhension dans nos rangs.

De fait, il est aujourd'hui difficile de mener des échanges clairs avec le gouvernement sur ces enjeux. À titre d'exemple, j'étais hier à l'Agence nationale de la cohésion des territoires pour une régie, dans le cadre du déploiement de la fibre. Nous avons adressé un courrier au premier ministre, que son directeur adjoint de cabinet a ensuite envoyé à une ministre, qui l'a transféré à un autre ministre, lequel l'a lui-même réadressé à un troisième. Quelque part, quelque chose ne fonctionne pas.

Vous avez posé la question des dispositifs, notamment de l'éducation de la population. Dans cette perspective, le travail de proximité n'a pas forcément vocation à être encadré, dans la mesure où il intervient déjà grâce à une culture partagée entre les grandes municipalités, les grandes communes, les départements, les associations d'élus, les entreprises.

Madame Darrieussecq, votre analogie entre entreprises et collectivités locales est très pertinente, tant l'effet de taille joue. De même, vous avez raison de mettre en lumière les liens numériques entre les différentes collectivités. Par ailleurs, je serais tenté de dire que dans le cadre de la cybersécurité, il n'y a pas une bonne échelle unique, mais des échelles différentes, selon la façon dont le sujet est abordé. Chacun des échelons suit une logique qui lui est propre et la construction législative est confrontée à cette difficulté de devoir raisonner de manière multiscalaire sur un sujet donné. De fait, il est extrêmement difficile de mettre en place une adaptabilité.

Dans ce domaine, il me semble pertinent de s'inspirer de l'expérience du New Deal Mobile, qui a embarqué les services de l'État, en coprésidence avec les présidents de département et de région, dans des équipes projets, qui nous ont permis de travailler ensemble. Je salue à ce titre le travail bidirectionnel des préfets et regrette qu'il ne soit pas valorisé à sa juste mesure. Il pourrait être approprié de reconstruire quelque chose qui embarque les uns et les autres, de manière réellement opérationnelle.

Ensuite, nous devons nécessairement aborder le principe de réalité en matière de ressources humaines. Dans le département du Puy-de-Dôme, cinq agents se consacrent exclusivement à l'assistance des 8 000 ordinateurs des collèges du département, mais quatre d'entre eux doivent être aujourd'hui renouvelés. En conséquence, le service se retrouve amputé et nous sommes contraints d'alerter les principaux de collèges. Le principe de réalité concerne également la dimension financière. La mutualisation peut être utile en fonction des situations, mais au-delà, l'essentiel concerne l'efficience des investissements. Vos auditions devraient vous permettre d'identifier les points qui permettront d'initier des dynamiques d'entraînement.

Madame Saint-Paul, vous nous avez interrogés sur le seuil des 30 000 habitants. La logique d'harmonisation s'applique aux communes. Il a également été fait mention dans vos questions de la nécessaire acculturation numérique des acteurs. Nous sommes tous frappés d'illectronisme à un moment ou un autre. Qui, dans cette salle, n'a jamais proféré une bordée d'injures parce qu'il n'arrivait pas à valider tel ou tel questionnaire en ligne ?

Cette acculturation doit être initiée par les élus. Une collectivité a par exemple mis en œuvre des messages pièges, à titre de test. La personne qui se fait hameçonner lors de l'exercice se voit ainsi proposer une petite formation. J'ai moi-même été piégé une fois par un hameçonnage malveillant.

En conclusion, au-delà des enjeux numériques dans leur globalité, la cybersécurité est révélatrice des interrogations et des vulnérabilités de notre société. À ce titre, je vous remercie une fois encore pour votre invitation et vos questions, qui confortent notre engagement dans ce domaine, mais également notre volonté d'échanger régulièrement avec les parlementaires. Comme j'ai déjà pu l'évoquer avec certains d'entre vous, il serait certainement utile d'organiser plus régulièrement de tels échanges. De notre côté, nous sommes demandeurs, en tout état de cause.

M. Éric Bothorel, rapporteur général. Pour rebondir sur les propos de Mme Nebbula, il me semble que le monopole de la violence légitime, qui caractérise les missions régaliennes en matière de sécurité, ne peut pas totalement s'appliquer aux enjeux cyber, puisqu'elle concerne la violence physique. De fait, dans le domaine cyber, les actions d'assistance et de soutien sont majoritairement assurées par des acteurs du privé. La caractérisation même de l'activité de la cybercriminalité et la réparation des dommages subis ne peuvent donc pas reposer uniquement sur l'État, ni sur les collectivités.

Monsieur Sauvade, je souhaite revenir sur les zones touristiques, qui ne peuvent pas être envisagées sans penser aux zones littorales. Pourquoi n'avez-vous voulu réaliser qu'une expérimentation sur la couverture numérique du territoire, alors qu'un dispositif bien plus efficace aurait pu être envisagé dans le cadre du projet de loi sur la certification ?

Vous avez tous souligné par ailleurs que les dispositions du projet de loi devraient être progressives, supportables financièrement et techniquement. Comment y parvenir ? Quelles sont vos propositions concrètes, afin que la mise en œuvre de NIS 2 soit graduelle et progressive ?

M. Thomas Gassilloud (EPR). Je souhaite vous faire part de trois messages. D'abord, la subsidiarité n'équivaut pas au désengagement de l'État. Nous avons besoin de tout le monde pour faire face globalement à la menace. La responsabilité de l'État consiste aussi à indiquer qu'il ne peut pas tout faire à lui seul ; je partage en cela les propos du rapporteur.

Deuxièmement, nous entrons progressivement dans un nouveau monde de conflictualité. À ce titre, notre objectif ne concerne pas uniquement la confiance dans l'économie numérique pour le développement des affaires, mais aussi l'efficacité de notre résilience globale. Je répète que le changement culturel me semble aussi important que la norme.

Enfin, il existe un besoin de clarification dans l'organisation territoriale, concernant les questions de défense. Il faut à ce titre s'appuyer sur un échelon de cohérence dans les territoires, qui pourrait se situer à l'échelle régionale. Par ailleurs, dans ma région, le préfet délégué à la sécurité et à la défense peut jouer ce rôle.

M. Denis Masséglia (EPR). Je partage nombre des questions qui ont été posées par mes collègues et il ne me semble pas opportun de les reformuler. Je tiens également à souligner le travail du Sénat sur l'article 5 *bis*, qui a été intégré dans un premier temps en commission, et qui permet de fournir des moyens financiers et humains aux collectivités territoriales. Je tiens également à remercier l'ensemble des élus aujourd'hui présents pour échanger avec nous sur cet enjeu essentiel.

Vous avez par ailleurs souligné l'intérêt d'un guichet unique à l'échelle gouvernementale. Certains d'entre nous le demandent depuis 2017 et je regrette que l'Assemblée nationale ne se saisisse pas suffisamment de ces sujets de transformation et de transition numérique. Notre société fait en effet face à deux transformations majeures : la transformation écologique et la transformation numérique. N'oublions pas l'une des deux en chemin.

M. le président Philippe Latombe. Nous n'avons pas parlé d'un « éléphant dans la pièce », qui est également issu de l'avis du Conseil d'État. Il concerne les sanctions, que nous n'avons pas abordées jusqu'à présent. En conséquence, je souhaiterais connaître votre point de vue à ce sujet.

Le Conseil d'État estime qu'il y aurait une forme d'iniquité entre le secteur privé le secteur public si le texte n'intégrait pas de sanctions pour le secteur public. Nous pouvons certes comprendre les contraintes budgétaires existantes, mais l'objet consiste bien ici à rehausser le niveau de cybersécurité. Dans le cadre du règlement général sur la protection des données (RGPD), les collectivités se sont assez rapidement conformées aux obligations et n'ont pas été celles qui ont dû subir le plus de sanctions.

Dans la mesure où certaines collectivités et EPA ne montent délibérément pas en puissance en matière de protection cyber, ne faut-il pas envisager des sanctions – y compris non financières – pour les obliger à se conformer aux règles, au-delà du *name and shame* prévu par l'Anssi ?

Mme Constance Nebbula. Monsieur le rapporteur, vous nous avez interrogés sur nos propositions financièrement et techniquement supportables, ainsi que sur leur délai de mise en œuvre. De notre côté, nous estimons que trois ans suffisent. Les régions demeurent des structures consistantes, dotées de budget et de SI structurés ; nous ne sommes pas les plus à plaindre. Le financement concerne pour nous l'outil des CSIRT ; à titre d'exemple, la région Pays de la Loire a mis en place ses propres dispositifs d'accompagnement cyber à partir de ses propres budgets.

En revanche, le financement doit intervenir à partir du moment où il existe une initiative nationale, qui est la même pour tous les acteurs et qui a vocation à être pérennisée sur tous les territoires. Nous souhaitons donc une clarification des outils, qu'il s'agisse de l'outil CSIRT ou de l'outil campus cyber.

S'agissant de la collaboration avec l'État, nous considérons que la préfecture régionale représente la bonne échelle pour échanger et travailler sur les sujets qui nous concernent, à condition que les interlocuteurs soient réceptifs. En revanche, en région, l'Anssi est très efficace ; tous les retours dont nous disposons sont concordants.

S'agissant des sanctions, je me souviens de la norme RGAA (référentiel général d'amélioration de l'accessibilité) sur l'accessibilité numérique, qui avait été votée il y a dix ans dans le cadre d'une loi sur le handicap. Elle oblige les collectivités territoriales à proposer des sites internet accessibles, afin de répondre à la réglementation sur l'accès à l'autonomie. Aujourd'hui, moins de 5 % des collectivités respectent cette norme sans pour autant subir de sanctions. Les collectivités qui commencent la démarche le font sur le seul fondement de leur volonté. À Angers, nous avons ainsi investi plusieurs centaines de milliers d'euros. Dans le même ordre d'idée, l'open data est censée être une obligation légale, mais seulement 16 % des

collectivités la respectent, sans que les autres ne soient pour autant sanctionnées. Ces exemples attestent de fait de l'absence de suivi politique sur les sujets numériques.

Forte de ce constat, j'aurais tendance à penser que la sanction n'est pas une bonne idée. Inversement, il faut trouver des manières d'inciter les collectivités à agir, à travers une ambition politique nationale sur les sujets numériques. Je précise que ces propos concernent plus les petites collectivités que les régions ou les métropoles.

Mme Marlène Le Dieu De Ville. L'accessibilité numérique est un sujet qui évolue, enfin. La loi de 2005 concerne l'accessibilité de tous les outils, non seulement les sites internet, mais plus largement les outils numériques utilisés par des collectivités. À partir du mois de juin 2025, des contrôles de conformité seront menés sur l'ensemble des collectivités et des entreprises soumises au RGAA et des sanctions financières seront appliquées.

Au-delà, s'agissant du texte de loi, il est très difficile d'envisager des sanctions financières, même à trois ans. Il faut d'abord accompagner la montée en compétences des collectivités sur NIS 2 et poser des jalons adaptés à chaque degré. Les métropoles estiment par exemple que le délai de trois ans sera trop court en raison de la complexité du code des marchés publics, qui ne permet pas de changer de prestataire facilement. De fait, des aménagements seront forcément nécessaires, dans le cadre d'une progressivité souhaitable. D'éventuelles sanctions financières ne peuvent intervenir qu'en cas de mauvaise volonté manifeste de la collectivité.

Ensuite, l'enjeu des ressources humaines est effectivement incontournable, mais il est tout aussi difficile de trouver des solutions. Dans mon intercommunalité, notre RSSI, qui avait débuté en alternance va bientôt partir et il sera difficile de le remplacer. Nous ne pouvons pas payer un RSSI, un expert ou un ingénieur à la hauteur de ce qu'il peut prétendre dans le privé.

La soutenabilité financière ne peut être atteinte qu'à l'aide d'un véritable accompagnement financier, semblable à celui que nous avons connu avec le parcours cyber du plan France Relance. Il sera notamment nécessaire de travailler sur un véritable audit.

M. Alexandre Ventadour. Nous sommes très attachés à l'exemption de sanctions pour les régions et les collectivités territoriales, d'abord parce que nous ne maîtrisons pas toujours directement les SI – qui peuvent être sous-traités – et ensuite parce que nous ne disposons pas des mêmes ressources que les entreprises, quelle que soit leur taille, pour recruter les personnes les plus à même de sécuriser nos infrastructures. Nous conduisons déjà des démarches volontaires de sécurisation, avec nos moyens actuels.

Nous portons en notre sein la responsabilité vis-à-vis de nos populations. *De facto*, nous sommes concernés par tout ce qui pourrait porter préjudice aux citoyens ou aux entreprises. S'il s'agit d'enjoindre une région ou une collectivité à se mettre en conformité, il suffit que la chambre régionale des comptes intervienne. Nous ne pensons pas qu'une sanction financière sur un chiffre d'affaires, qui n'existe pas dans notre cas, constituerait le bon outil. En revanche, nous sommes en mesure d'accepter la mise en place d'audits et la nécessaire mise en conformité, à la suite des résultats de cet audit, dans un laps de temps donné, qui pourrait être par exemple de trois ans. Non seulement nous l'acceptons, mais nous sommes prêts à l'encourager.

Enfin, je considère que la cybersécurité demeure la prérogative de l'État. Les agressions ont évolué depuis un certain temps. Les maux causés de manière virtuelle par les cyberattaques peuvent également se retranscrire de manière assez physique. Dès lors, la protection de la sécurité demeure l'apanage du régalien. En résumé, nous militons pour une exemption de la sanction, mais nous ne préconisons pas une exemption de la responsabilité des collectivités. Cela doit se traduire par un audit, auquel nous nous conformerons, bien évidemment.

M. Michel Sauvade. Comment pouvons-nous agir, concrètement ? Il s'agit de poursuivre les travaux communs, de nous réunir autour d'une même table, sur le plan national et local. Jusqu'à présent, nous avons été écoutés, mais nous n'avons pas été entendus.

Financièrement, nous payons l'absence d'étude d'impact, non seulement l'étude d'impact à date, mais également sur la trajectoire financière, pour autant que nous puissions l'évaluer en fonction de l'augmentation des menaces et des autres vulnérabilités. Simultanément, nous ne disposons pas non plus d'indicateurs ; nous savons uniquement que les moyens ne seront pas à la hauteur de ce que nous attendons. À ce titre, ce sujet doit s'envisager plus largement dans le cadre de la décentralisation des moyens, au plus près du terrain. Cette piste peut sans doute être explorée, à la lumière des propos échangés aujourd'hui par les uns et les autres.

Sur le plan technique, les enjeux de la formation sont patents. Madame Le Dieu De Ville a également mentionné à juste titre les difficultés concernant les recrutements ou les salaires. Dans ce domaine, une véritable réflexion doit être conduite sur notre capacité à nous « muscler » en matière numérique. Cette réflexion doit être conduite, me semble-t-il, à la fois sur le plan national, mais aussi régional. À une certaine époque, dans le domaine du numérique, la France était particulièrement dynamique, en pointe. Cela n'est plus le cas, désormais.

S'agissant de la progressivité, notre réponse est très claire. De notre côté, nous imaginions une marge de progression dans un délai de trois à cinq ans. Cependant, l'Anssi nous a expliqué que la progressivité ne peut pas être prise en compte dans le cadre de la transcription de directives européennes. Nous sommes donc bloqués sur ce point, ce qui est regrettable, dans le cadre d'une réflexion sur l'évaluation et la sanction.

Le simple fait de se poser la question revient déjà s'interroger sur l'efficience de la mise en œuvre de la loi et révèle l'ambiguïté de sa mise en application. En effet, le questionnement sur la sanction traduit quelque part un échec collectif à embarquer tous les acteurs sur un sujet qui est pourtant essentiel. De son côté, sur d'autres sujets, la Commission nationale de l'informatique et des libertés (Cnil) a prononcé des sanctions lorsqu'il existait une mauvaise volonté manifeste. Or de tels cas demeurent heureusement assez rares. L'AMF ne peut pas se satisfaire d'un cadre de sanctions qui, de toute façon, ne résoudra pas les problèmes.

M. le président Philippe Latombe. Je vous remercie pour vos réponses, votre liberté de ton et d'expression lors de cette table ronde, laquelle ne constitue que le début de nos travaux. Nos interactions se poursuivront.

La séance est levée à onze heures cinquante-cinq.

Membres présents ou excusés

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Réunion du jeudi 15 mai 2025 à 9 h 30

Présents. - M. Éric Bothorel, Mme Geneviève Darrieussecq, Mme Virginie Duby-Muller, M. Thomas Gassilloud, M. Philippe Latombe, M. Denis Masséglia, M. Jacques Oberti, M. René Pilato, Mme Laetitia Saint-Paul, M. Arnaud Saint-Martin.