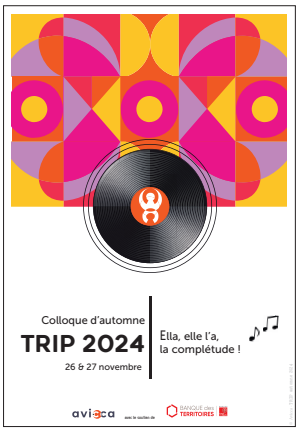

TRIP D'AUTOMNE 2024

26 et 27 novembre

Table ronde 3
NIS2, « the final countdown"

Animation :

- **Mickaël AUDEGOND**
  Conseiller communautaire, usage du numérique et stratégie digitale, communauté urbaine d'Arras
- ,

Intervenants :

- **Damien MICHALLET**
  Président - CSNP (Commission Supérieure du Numérique et des Postes)
- **François DÉGEZ**
  Chef de Division Coordination Territoriale - ANSSI
- **Hugues FOULON**
  CEO - Directeur Général - Orange Cyberdéfense
- **Stéphane VANGHELUWE**
  Directeur Général des Services - SITIV - Déclic

Mickaël AUDEGOND, Conseiller communautaire, usage du numérique et stratégie digitale, communauté urbaine d'Arras

Nous commencerons cette matinée par le sujet essentiel de la cybersécurité au sein de nos entreprises et de nos collectivités territoriales. Aujourd'hui, c'est un focus sur la directive européenne Network Information and Security, connue sous l'acronyme NIS2, opus de mise à jour du texte de 2016. Le cybercrime capitalise sur notre dépendance aux nouvelles technologies, et en même temps la cybersécurité est souvent perçue comme une contrainte. Le

développement en volume et en sophistication des attaques sur nos systèmes met sur le devant de la scène l'urgence de solidifier la résilience des infrastructures de nos entités. Nous allons nous poser plusieurs questions. En quoi la cybersécurité est-elle un enjeu crucial pour l'avenir de nos territoires ? Quelles conséquences en termes d'organisation et de stratégie au niveau national et surtout local ? Et enfin, la directive NIS 2 est-elle juste un texte de plus ou alors une opportunité collective de « cranter » et d'amener nos défenses à des niveaux suffisamment forts pour parer les offensives du cybercrime ? Le 17 octobre dernier, l'ensemble des États membres de l'Union européenne devaient l'appliquer et mettre en musique, je cite, « des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne » Seuls trois pays sont parvenus à cette échéance. La France a raté ce rendez-vous. Certes, la dissolution n'a pas aidé les choses. A nouveau saisie par le Gouvernement, le Sénat a repris les travaux entamés avant l'été sans que le texte soit encore inscrit à l'ordre du jour du Parlement. Nous avons donc souhaité éclairer les enjeux prévisibles de cette future transposition en associant ceux qui construisent le cadre et ceux qui proposent des solutions opérationnelles pour y répondre.

Tout d'abord, je vais demander à chacun comment il entend la liaison entre la cybersécurité et les territoires, notamment avec nos collectivités ?

Monsieur MICHALLET, vous êtes sénateur et président de la Commission supérieure du numérique et des postes. La CSNP s'est saisi de la transposition de NIS2 dans le rapport de Madame la députée Anne LE HENANFF, le 3 octobre dernier. Quelle est l'angle d'analyse et l'enjeu d'aborder un tel sujet pour une commission comme celle que vous présidez ?

Damien MICHALLET

La Commission supérieure du numérique et des postes (CSNP) a été saisie en mai 2024 par l'ANSSI sur le projet de loi résilience avant que le texte soit publiquement présenté. Nous avons rendu un avis sur le texte fin mai 2024. Avec Anne LE HENANFF nous avons mené ce travail ensemble. Nous avons considéré que NIS 2 constituait un enjeu majeur pour nos entreprises et pour nos collectivités en tout cas pour les entités concernées. Nous avons eu un angle d'attaque assez simple, avec un esprit très sénatorial, c'est-à-dire pragmatique, mais en essayant d'être quand même transversal. Nous avons examiné les implications concrètes de cette directive sur les différentes entités et sur les différents secteurs qu'elle touche, infrastructures essentielles comme énergie, santé, télécommunications ou fournisseurs de services numériques. L'objectif

était d'évaluer comment cette transposition pouvait améliorer la sécurité tout en rendant sa transposition possiblement opérationnelle pour les entreprises et les collectivités territoriales concernées. Pour une commission comme la nôtre, l'enjeu est double. Tout d'abord de garantir un cadre législatif adapté à la spécificité française malgré la transposition, sans alourdir les obligations des acteurs économiques et des collectivités locales. Ensuite nous avons veillé à ce que le texte soit adapté à la réalité notamment des nouveaux acteurs qui vont être concernés et d'aménager les délais de la transposition. Pour rappel, NIS1 concernait 600 entités alors que NIS2, selon l'étude d'impact, concerne 15.000 entités. Donc il était clair que le paradigme s'en voit modifié. Il fallait absolument que nous ayons une adaptation à la réalité des nouveaux acteurs. Alors, nous avons fait des recommandations. Nous voulions absolument que NIS2, malgré tout ce qu'elle amène de structurant et peut-être de contraintes, soit aussi une opportunité et non pas une occasion de plus de surtransposer et d'alourdir ce que nous savons généralement bien faire, nous, les législateurs.

Mickaël AUDEGOND

François DÉGEZ, vous êtes chef de division coordination territoriale de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). L'ANSSI est d'abord regardée comme le bras armé national de l'État dans le domaine de la cybersécurité. Mais pouvez-vous nous présenter rapidement aussi la structure territoriale de l'ANSSI et les initiatives qu'elle appuie sur les territoires et qui s'articuleront plus tard avec les mesures NIS2 ?

François DÉGEZ

A l'ANSSI, nous nous rendons bien compte depuis quelques années que le risque numérique est partout. Il touche absolument tous les territoires. Et de fait, il a paru évident que l'ANSSI, qui était historiquement une agence très technique d'experts auprès de l'État, devait s'adapter à cette nouvelle donne. D'une part, il y a eu en 2016, Cybermalveillance, le GIP qui a été créé pour aller au plus près des citoyens. Et en décembre 2015, l'ANSSI, dans sa réflexion territoriale, a choisi d'implanter dans les régions, là où se passe la plupart de la réflexion de l'organisation territoriale et de la vie économique, des délégués régionaux, qui ont principalement trois grandes missions. Une première mission qui est de faciliter et de créer toutes les opportunités de manière à développer la cyber-résilience dans les territoires, donc d'encourager toutes les initiatives, les connaître, etc. Une deuxième mission qui est vraiment une mission de « capteurs », pour ramener auprès de l'ANSSI les techniciens de haut vol, les sujets de préoccupation des territoires, de

manière à ce que dans leur préoccupation et dans leur préconisation, ils en tiennent compte. En troisième lieu, nous sommes les ambassadeurs, les points de contact et puis les relais de l'ANSSI dans ses différentes actions, que ce soit auprès des OIV, que ce soit dans la contribution, la coordination, l'action de l'État, que ce soit dans les discussions et toutes les propositions que nous pouvons avoir avec ceux qui sont des acteurs sur les territoires et qui réfléchissent aux politiques publiques. Et puis nous sommes aussi les relais, les points de contact lorsqu'il y a de grands événements d'origine cyber. Nous sommes répartis sur le territoire depuis octobre 2022 à hauteur de 1 à 2 délégués par région, y compris pour les territoires d'outre-mer.

Mickaël AUDEGOND : Hugues FOULON, vous êtes directeur général d'Orange Cyberdefense, qui est une des entreprises majeures du secteur et filiale d'un opérateur que nous ne présentons plus. Les opérateurs télécoms ajoutent de plus en plus des services de cybersécurité à leur offre. Cette montée en puissance est-elle le meilleur vecteur pour diffuser une expertise, une culture de la cybersécurité sur tous les territoires ?

Hugues FOULON

Je vais complètement dans le sens de ce qui vient d'être dit. Autant le cadre, les enjeux, la réglementation sont fixés par l'instance publique et orchestrés par l'ANSSI, autant la réponse est éminemment privée. C'est-à-dire que les enjeux de cybersécurité sont traités par le privé. Songez aux JO qui viennent de se passer, si Orange, si BNP, si SNCF, si Air France avaient été durement attaqués, les Jeux auraient été un échec. Et pour faire écho à ce qui vient d'être dit, Orange Cyberdefense qui est une filiale de plein exercice avec 3.000 experts dédiés à la cybersécurité, sa propre marque, sa propre équipe, son propre siège, est la seule entité sur le territoire national à avoir 100 experts en cybersécurité à Lille, 100 experts en cybersécurité à Lyon, 100 experts à Marseille, à Toulouse, à Bordeaux, à Rennes, à Strasbourg. Nous sommes au plus près des territoires justement pour adresser ces sujets-là, que ce soient les collectivités, les PME, le tissu industriel, puisqu'aujourd'hui, près des deux tiers des cyber-extorsions, ce qu'on appelle les fameux ransomware, touchent des PME. Les grands groupes sont globalement bien protégés, néanmoins les PME qui font partie de leur supplychain ne le sont pas. Il y a un décalage considérable entre la perception et la réalité. Nous avons fait un sondage : 90% des patrons de PME pensent qu'ils sont bien protégés. Or, c'est très loin d'être le cas. Il y a un écart quantique entre le niveau de cybersécurité, le niveau de protection nécessaire et la réalité. C'est vraiment un des enjeux majeurs dans la cyberdéfense.

Mickaël AUDEGOND : Stéphane VANGHELUWE, vous êtes DGS du SITIV, membre du conseil d'administration de l'association Déclic. Vous représentez un organisme public de services informatiques mutualisés, principalement autour du Grand Lyon. Depuis quand voyez-vous la question de la cyber devenir une demande importante de la part de vos adhérents ? Et comment cette prise de conscience se traduit-elle sur le terrain ?

Stéphane VANGHELUWE

Déclic, c'est l'acteur associatif des agents du dernier kilomètre. Nous sommes là pour délivrer du service numérique au secrétaire de mairie sur les territoires. Ce sont 2.000 agents sur le territoire. Notre unique enjeu est de développer des services numériques. Donc la cybersécurité est au cœur de nos enjeux. 80% de nos structures ont mis cet enjeu numéro 1 dans leur feuille de route. Peut-être que NIS2 est l'opportunité de mettre en valeur encore plus cette nécessité d'une gouvernance de nos élus sur le terrain, pour s'intéresser au sujet une fois par an et mettre en œuvre un plan d'action suivi. Avec les spécialistes, nous avons encore une fois des OPSN qui sont des ESN publics un peu partout sur le territoire.

Mickaël AUDEGOND

Vous voyez effectivement que la présentation initiale montre bien les deux thèmes de notre présentation d'aujourd'hui. Nous avons le cadre réglementaire, puis différentes expérimentations. Monsieur le sénateur, Damien MICHALLET, les débats du projet de loi de transposition n'ont pas encore démarré, mais votre instance bicamérale a d'ores et déjà présenté et proposé 32 recommandations publiques avec une attention particulière sur les impacts locaux. Pouvez-vous nous présenter dans les grandes lignes votre approche ?

Damien MICHALLET

NIS2 a été adoptée en décembre 2022 et son objectif est de renforcer au niveau européen notre approche de la cybersécurité. En France, elle aurait dû être transposée le 17 octobre 2024, puis la dissolution a bousculé le planning. NIS2 a été présenté en Conseil des ministres par la ministre Clara CHAPPAZ, que nous avons auditionnée il y a 15 jours. Il faut bien avoir en tête ce que cette directive de mise en place de process cybersécurité est au niveau de nos entreprises et au niveau de nos collectivités. Ce point est important et il nous concerne tous. NIS2, c'est toutes les

collectivités de plus de 30.000 habitants qui sont touchées, qui sont classées comme entités essentielles ou importantes et qui devront adapter leurs process, leurs systèmes d'information, au standard de la cybersécurité tel qu'imposé par cette directive européenne. Mais il y a aussi toutes les petites collectivités qui sont directement ou indirectement touchées. Indirectement parce que nous avons des liens avec notre interco, parce que nous avons des services mutualisés, et bien qu'elles soient exclues de ce périmètre, elles seront de toute façon, encore une fois, tellement dépendantes des intercos ou des prestataires qui peuvent être soumis au niveau des intercos qu'elles sont indirectement dans le spectre. Ensuite, il y a des collectivités qui n'ont pas forcément 30.000 habitants mais qui adressent des secteurs comme l'eau ou la gestion des déchets qui sont inclus dans la directive NIS2, ce qui veut dire que des petites collectivités de quelques centaines d'habitants sont éligibles à la directive NIS2. Donc, les collectivités territoriales vont avoir à faire face à de vrais défis. J'ai été vice-président au département de l'Isère, vice-président à l'agglomération Porte de l'Isère, une grosse agglomération dans l'Isère où nous avions des schémas, des process, des équipes informatiques, mais pour autant, nous étions plutôt en tension et pas toujours bien équipés. Ce qui veut dire que nous allons avoir un vrai sujet de ressources pour les grandes mais notamment pour les petites structures. Il va aussi y avoir un sujet de compétences. La cybersécurité, c'est un sujet qui explose. Nous allons avoir un sujet de ressources autour de la cybersécurité et cela complique sa mise en œuvre. Alors, nous avons d'excellentes entreprises françaises, locales et nationales qui vont pouvoir nous accompagner. Pour autant, nous avons là une vraie difficulté à laquelle devront faire face nos entreprises comme nos collectivités. À la CSNP, dans les recommandations que nous avons pu faire, il est clair que nous mettons en place des dispositifs d'accompagnement financier, mais également des dispositifs techniques en s'appuyant sur l'ANSSI, et également sur les préfectures, et notamment à destination des collectivités territoriales qui en auraient besoin.

Il y a aussi un sujet que j'ai découvert dans le cadre des auditions de la CSNP. Il faut que nos collectivités partent vers des solutions SaaS un peu plus robustes d'un point de vue cybersécurité. Mais le SaaS n'est pas éligible à l'investissement, mais au fonctionnement. Ce qui pose un problème fondamental dans cette période de tension. Alors, il faut que nous réussissions d'une manière ou d'une autre, au travers de la loi ou par décret, autour de NIS2, de modifier cet angle-là qui pourrait être un vrai catalyseur pour les collectivités. Ensuite, il est indispensable de former les élus et les équipes techniques aux enjeux des cyberattaques. Il arrive parfois que dans nos collectivités, l'aspect informatique soit un peu mis de côté, parce que politiquement, ce n'est pas un vrai levier. Mais pour autant, l'enjeu cyberattaque est tel qu'il faut absolument que nous

sensibilisions nos élus comme les équipes techniques. Alors, nous avons mis en exergue un certain nombre de défis. Il y a donc là un vrai sujet de communication.

Nous avons également un sujet sur les délais de mise en conformité. A la CSNP, nous recommandons un plan en trois étapes qui permet un peu d'étaler les délais. D'abord, la sensibilisation par la communication. Comment sensibilisons-nous les élus et les industriels au sujet des cyberattaques et de NIS2 ? Puis, le contrôle et les sanctions.

Nous avons fait 32 recommandations. Je vais vous parler des cinq qui me semblent être les plus importantes et vous dire dans quel esprit nous avons accueilli cette directive à la CSNP. Il est très important de mener la communication de NIS2 différemment que celle de certains dispositifs, tel le RGPD. Dès que le législateur aura fini son travail, il faut absolument que nous ayons une campagne forte pour informer nos entreprises comme nos collectivités locales. Et puis, nous avons proposé dans nos recommandations de créer un label NIS2 pour dire « Je suis NIS2 ». Cela a plusieurs intérêts, celui de coordonner la communication, mais aussi d'avoir et de créer une famille, un sentiment d'appartenance à la famille NIS2 qui peut mobiliser les acteurs. Ensuite, spécifiquement sur les collectivités, il convient de renforcer la présence de l'ANSSI dans les territoires, en région, avec des experts dédiés, de clarifier aussi le rôle des équipes d'intervention en cybersécurité, les CSIRT régionaux. Et puis, évidemment, il y a une notion de financement, parce que tout cela va avoir un coût. Il faut que nous réussissions à accompagner via des fonds publics ou des soutiens ciblés, les petites communes pas ou mal équipées. Un point important, la simplification administrative : il ne faut pas que NIS2 soit une occasion supplémentaire d'alourdir le dispositif, tant au niveau des collectivités qu'au niveau des industriels. Il faut que nous soyons dans une simplification. Par exemple avec un seul guichet pour déclarer les incidents, avec des formulaires simples et le moins de formulaires possible pour rendre cette directive facilement applicable, et, encore une fois, que nous puissions mobiliser sans perdre et sans alourdir plus que nous le faisons déjà. Par ailleurs, les législateurs ont tendance à surtransposer. Or, la recommandation de la CSNP n'est pas de surtransposer, mais d'être dans une application stricte de la directive européenne, parce que nous avons NIS2, la CSRD, la dématérialisation qui arrive pour nos entreprises, … Il ne faut absolument pas que nous créions un nouveau dispositif. Nous sommes très insistants là-dessus.

Ensuite, il faut s'assurer que les exigences ne sont pas disproportionnées par rapport à la taille de l'entité concernée. Il faut donc réussir à allier la taille et les enjeux, et derrière les notions de contrôle et de sanction, adaptées aux entités et à leur taille.

Vient ensuite la notion de mutualisation qui est absolument nécessaire : mutualisation dans la santé, au niveau de l'eau via les syndicats intercommunaux, au niveau des infrastructures. Pour limiter les coûts, la mutualisation est fondamentale. NIS2 n'est pas un énième « truc » qui vient de Bruxelles, NIS2 c'est de la politique. Le numérique, c'est d'abord de la politique et NIS2 en est la preuve. Il faut que nous nous organisions et que face aux cyberattaques, nous soyions plus résilients. Parfois, il faut un peu accompagner la dynamique et cela passe par la loi. Et NIS2 est là pour rendre nos entreprises plus compétitives, pour rendre nos collectivités plus fortes face aux cyber-risques.

Mickaêl AUDEGOND

Effectivement, ces recommandations nous donnent des clés de lecture par rapport à un texte qui n'est pas forcément toujours simple à appréhender. En nous référant au RGPD, qui est la réglementation européenne la plus connue en France, tout ce que nous pouvons souhaiter, c'est que NIS2 soit aussi connue d'ici quelques années. Cela voudra dire aussi qu'elle est appliquée et qu'elle est dupliquée. Quant à la transposition, notre Premier ministre nous l'a promise la semaine dernière. François DÉGEZ, l'ANSSI s'est fortement impliquée dans un vaste échange préalable avec les territoires et les associations d'élus. Et ces échanges ont été très appréciés pour mieux définir les entités qui seront concernées et les modes opératoires qui devront être mis en place pour rehausser la cybersécurité. Pouvez-vous nous expliquer le plus simplement possible les conséquences pour les entités finalement concernées et comment interagiront-elles à l'avenir avec l'ANSSI ?

François DÉGEZ

Je vous rappelle que NIS2 vient après NIS1, que NIS1, c'était 600 entités, et que nous passons à plusieurs milliers. La grande nouveauté, c'est qu'il y a un régime de sanctions, à l'instar de ce qu'était le RGPD, alors que NIS1 n'avait pas cette dimension-là. De plus, NIS2, c'est aussi une extension de tous les mécanismes de coopération entre États membres en cas de crise, puisque cela institue, de par la loi, le réseau des CERT, des CERT nationaux. Je ne rentre pas pour l'instant dans le dossier des CSIRT-CERT territoriaux. Et puis, NIS2 réaffirme l'importance du rayon

d'alerte, puisque parmi les obligations, il y a un certain nombre de questions qui ont trait à la notification des incidents et au partage d'informations. A la différence de NIS1 où c'était l'État qui désignait les OSE, dans NIS2, dès lors que vous remplissez un certain nombre de seuils et de critères, que vous êtes et que vous appartenez à ces secteurs, vous êtes, d'entrée de jeu, concernés. Autre changement et détail, c'est que dans NIS1, il fallait que chaque entité identifie son système d'importance à protéger, alors que, dans NIS2, changement de principe, c'est l'ensemble du système qui est concerné par défaut. Je dis par défaut parce que vous avez la possibilité, si vous créez une analyse de risque, d'écarter certains bouts de système s'il est démontré que, par rapport aux enjeux de fonctionnement de l'entité, ils sont d'une importance secondaire. L'objectif, c'est de rajouter aussi un niveau de défense, un socle de règles harmonisées au niveau de l'Europe, adapté au niveau de menaces ainsi qu'aux spécificités sectorielles. Et puis, enfin, NIS2 introduit un régime de proportionnalité qui n'existait pas avant, puisque nous distinguons les secteurs hautement critiques, qui doivent avoir des mesures de protection très forte, et un secteur seulement critique, pour lequel nous pouvons nous satisfaire de mesures de base.

Un petit rappel rapide, juste pour vous faire cibler qu'il y a une grande nouveauté dans NIS2 au travers des secteurs concernés, qui sont relativement classiques comme l'infrastructure des marchés financiers, mais l'eau, les eaux usées, c'est nouveau. L'infrastructure numérique, ce n'est pas nouveau. Le secteur bancaire, l'espace, l'énergie, les transports, non plus, mais l'administration publique, ça l'est. Et dans administration publique a été introduit le fait qu'il y a les administrations nationales et locales. Il est laissé à chaque État membre le soin de définir ce qu'est une administration locale. Quelles obligations pour les entités ? Le partage d'informations, la mise en place de mesures adaptées à la gestion du risque cyber, la déclaration d'incident. Parmi les premiers partages d'informations, et ce sont ceux sur lesquels nous serons sans doute le plus exigeants rapidement, c'est « déclarez-vous », car la directive dit que les entités doivent se signaler auprès du CERT national. Et puis enfin, c'est générique, la directive prévoit la capacité d'imposer des sanctions financières. Pour l'instant, dans le projet de loi qui a été remonté et qui a été déposé au Parlement, les collectivités territoriales et les administrations publiques ne sont pas dans le champ des entités susceptibles de faire l'objet d'une sanction. Le Conseil d'État estime que ce n'est pas forcément justifié, mais les parlementaires, dans leur infinie sagesse, qui ont le dernier mot, trancheront. Pour l'instant, c'est l'état des réflexions du projet de loi.

Revenons un peu aux collectivités territoriales, c'est le sujet qui vous intéresse le plus aujourd'hui. L'ANSSI a fait un petit panorama de la menace adaptée. Il y a maintenant un an et sur une période de 18 mois, l'ANSSI avait traité 187 incidents de cyber sécurité concernant les collectivités, représentant 17% du total des incidents signalés à l'ANSSI. Alors si vous faites rapidement une règle de trois, si vous comparez les 54.000 collectivités aux 3 millions d'entreprises privées, vous vous rendez compte quand même qu'il y a une légère surreprésentation des collectivités dans les victimes. Non pas que les collectivités soient entre guillemets plus des cibles, mais c'est peut-être plus révélateur d'un niveau de vulnérabilité générale par rapport au risque dit systémique et pas au risque stratégique. Les collectivités représentent 24% des attaques par « rançongiciels », les plus déstabilisantes pour le fonctionnement des entités.

La France a porté lors des négociations de NIS2 le fait que nous puissions intégrer des collectivités territoriales ainsi que certains établissements publics territoriaux. C'est ce que nous avons fait dans le projet de loi.

Alors en synthèse, si le projet de loi était voté tel quel aujourd'hui, l'estimation que nous avons au niveau des échanges avec la DGCL, c'est qu'il y aurait 2.479 collectivités et groupements et établissements rattachés qui seraient susceptibles d'être assujettis.

Enfin, une dernière information, les parcours de cybersécurité du plan de relance ont été très instructifs pour nous, de manière à mieux comprendre le fonctionnement des collectivités au travers de leur système d'information. Nous constatons que sur les 715 collectivités qui ont bénéficié d'un parcours, 50% des futures entités essentielles ont déjà été concernées, et 7% des futures entités importantes, notamment les communautés de communes. Dans le projet de loi, il faut retenir que les 992 communautés de communes françaises seraient assujetties au niveau « entités importantes », c'est-à-dire les entités qui sont un petit peu moins contraintes en termes d'objectifs à remplir. C'est un des sujets sur lequel la concertation a été la plus fructueuse. Dans le projet initial, nous étions partis de la fameuse barre des 30.000, (que je vais me dépêcher de tuer très vite) pour pouvoir l'appliquer à tout. Les associations d'élus ont attiré notre attention sur le fait qu'il y a des communautés de communes qui ont plus de 30.000 habitants. Effectivement, nous avons regardé, et pour autant elles n'ont pas de ville-centre assez importante pour disposer d'une DSI structurée. Nous avons travaillé la rédaction de manière à faire en sorte que ce soit la nature de l'EPCI qui soit au final le critère retenu dans le projet de loi. Les conseils régionaux et les

conseils départementaux ont de tels systèmes d'information et de tels enjeux en termes de services rendus aux concitoyens qu'il semblait évident qu'ils allaient rentrer dans la catégorie des entités essentielles. Je souligne que le raisonnement en termes d'outre-mer ou en termes d'Hexagone est identique. Avec la DGOM, nous nous sommes efforcés de faire que le projet de loi de transposition s'applique dans les mêmes termes. Les métropoles, les communautés urbaines, les communautés d'agglomération sont aussi des grosses structures dans lesquelles il y a beaucoup d'habitants et généralement il y a des DSI capées. C'est aussi ce que nous avons constaté dans le cadre du plan de relance. Et puis nous venons à ce fameux seuil des 30.000 habitants pour les communes. C'est comme cela qu'il fallait l'écrire, parce que c'était plus rapide à écrire que "toutes les communes qui ont une taille supérieure à la plus petite des entités essentielles". L'idée, c'est que les grosses EPCI, qui sont des entités essentielles, peuvent comprendre des communes de taille très importante. Par exemple la métropole nantaise a fusionné ses systèmes d'information avec la ville de Nantes, mais Rézé ou Saint-Herblain, qui sont des très grosses communes appartenant à la métropole de Nantes, ont une DSI autonome. Il serait absurde qu'elles ne soient pas assujetties à un certain nombre de régles d'écriture minimum, alors que Guéret, qui est une Communauté agglomération de tout juste 30.000 habitants, l'aurait été. Il faut retenir l'idée que les communes qui ont une importance, et donc a priori un système d'information aussi important que la plus petite des entités essentielles sont assujetties au même niveau. Et donc cette notion de seuil, finalement, c'est une facilité d'écriture.

Quelques points particuliers, les centres de gestion et les SDIS : les SDIS parce qu'ils sont essentiels dans le fonctionnement de la protection civile de nos citoyens et les centres de gestion parce qu'ils ont une organisation particulière qui a fait qu'ils ont souhaité être tous assujettis « entités essentielles ».

Et enfin, un petit point particulier. Il y a, et M. le sénateur l'a bien évoqué, un certain nombre de syndicats qui gèrent des activités qui sont ciblées par les annexes de la directive NIS : énergie, transport, etc. Aujourd'hui, il est écrit que le seuil pour assujettir ces syndicats est à 30.000 ; nous sommes conscients que nous l'avons fait par facilité d'écriture, mais nous pensons qu'il n'est pas adapté. Donc nous sommes vraiment ouverts à poursuivre le travail là-dessus. Si nous considérons que le seuil doit être élevé, il n'y a pas de contraintes, de contre-indications techniques valables. Là, c'est le terrain qui commande. Nous avons vraiment le souci d'être le plus proche de la réalité. Et cela m'amène juste à préciser une petite chose par rapport à ce que vous avez pu dire, monsieur le sénateur. Une petite collectivité qui gère de l'eau en particulier, n'est

assujettie dans le projet de texte actuel, que si c'est une commune ou une EPCI de plus 30.000 habitants. Donc les petites communes ne sont pas directement concernées quelques soient les activités qu'elles gèrent.

Ce n'est pas pour autant ainsi vous l'avez très bien dit, qu'elles ne le sont pas indirectement via les intercommunalités.

Cela m'amène à une seconde réflexion un petit peu plus générale. 99% au moins des communes, puisqu'il n'y a d'ailleurs que 272 communes qui font plus de 30.000 habitants, ne sont pas assujetties, ni au niveau EI, ni au niveau EE, directement. Elles le seraient en fonction de l'état de mutualisation de leur système avec les intercos. Par contre, 100% des EPCI le sont. Et quelque part, l'idée sous-jacente de tout cela, et la stratégie générale, c'était bien, dans l'esprit de la directive NIS2, d'arriver à déployer une cybersécurité de masse avec une deuxième préoccupation qui a déjà été évoquée à plusieurs reprises dans vos propos, inciter à mutualiser. Pour faire du numérique et de la cyber, il faut des compétences. Or les compétences c'est compliqué à assumer dans des collectivités pour lesquelles il n'y a que quelques centaines d'habitants, et donc que ce soit via les OPSN, via les agences techniques départementales, via d'autres structures, via les intercos, la mutualisation est le bon outil. L'idée c'est qu'il faut que tout le monde y passe. C'est ce qui a guidé notre plume. Alors, je l'évoque rapidement, nous avons fait cela en travaillant avec toutes les associations d'élus, les 11 associations d'élus qui sont dans la gouvernance de l'ANCT, y compris les élus d'outre-mer. Nous avons eu des contributions écrites d'un certain nombre d'associations. Grâce à des remarques d'Intercommunalité de France, nous avons adapté le texte de manière à ce que nous ne puissions pas avoir des communautés de communes qui soient EE, ce qui aurait été un trop gros effort pour elles.

Je vais poursuivre par le sujet de l'accompagnement, qui reste un gros sujet. Un certain nombre d'outils existent, qui sont à la disposition des collectivités, permettant de mesurer leur exposition aux risques, la fragilité de leur système de base de compte. Par exemple, MonAideCyber, et qui est un outil qui permet d'avoir une première démarche d'audit accompagné, avec quelqu'un qui vient expliquer aux élus, sur la base d'un diagnostic réalisé avec un outil construit par l'ANSSI, quelle pourrait être une démarche pour démarrer.

La directive NIS2 s'applique indistinctement aux collectivités et aux entreprises, c'est-à-dire que c'est la même règle, la même mécanique, modulo les problématiques de sanctions que j'évoquais

tout à l'heure. Ainsi mon espace NIS2 interesse tous les types d'entités et c'est une base d'informations qui se met à jour en permanence. Donc, connectez-vous, abonnez-vous à la newsletter ! Pour répondre aux besoins d'accompagnement plus ciblé pour les collectivités, nous allons travailler, pour faire la synthèse des 715 parcours cyber du plan de relance, de manière à les segmenter par rapport au type de collectivité concernées, les analyser par strate pour détecter les facteurs communs dans les plans d'action qui ont été proposés de manière à les partager avec les associations d'élus concernées par ces strates.

Nous sommes en train de constituer des groupes témoins au sein de toutes les associations d'élus, de manière à pouvoir, dans la phase actuelle de travaux réglementaires, avoir un échange le plus approfondi possible, afin que les contraintes propres aux collectivités puissent être remontées et qu'elles rentrent dans les processus d'arbitrage commun. Notre souhait est que ces groupes témoins et de contacts avec les élus puissent continuer à vivre après le processus législatif et réglementaire pour que l'accompagnement se poursuive dans la durée. Enfin, du point de vue financier, nous avions obtenu en 2024 que les sujets cyber puissent être intégrés à la DSIL. C'était dans la circulaire de 2024. Nous poursuivrons le dialogue avec le ministère en charge pour que cette possibilité soit maintenue.

Mikaël AUDEGOND

Des retours que nous avons, nous constatons que la question du numérique en général est souvent quelque chose de technique. Et que dans les entités, c'est souvent les DSI qui parlent au DSI finalement. Je vous rejoins aussi dans l'esprit de dire que c'est du politique et je me permettrai de rajouter que c'est aussi du stratégique

Hugues FOULON, Orange Cyberdefense a construit un écosystème de cybersécurité qui répondait initialement aux besoins des autorités et de grandes entreprises en France et en Europe disposant d'une direction informatique structurée. Avec NIS2, le marché va s'élargir considérablement. Comment voyez-vous la place d'une entreprise comme la vôtre dans ce nouveau contexte ? Et souhaitez-vous apporter votre réflexion sur le projet législatif en cours au regard de votre expérience dans d'autres pays européens ?

Hugues FOULON

Quelques points de réflexion à la suite de ce qui vient d'être dit. Le premier point, c'est qu'Orange Cyberdefense est une entreprise pan-européenne. Nous sommes présents dans une dizaine de pays européens, dont certains - comme la Belgique - ont déjà transposé NIS2. Nous accompagnons un certain nombre de collectivités et d'entreprises dans ces pays. Ces dernières ont commencé cette maturation, cette montée en gamme des enjeux cyber. Nous avons aussi l'habitude d'accompagner les collectivités locales en France, les forces de police, les hôpitaux, notamment pendant et après le Covid, durant lequel ils ont été durement attaqués. C'est vraiment une expertise de proximité, c'est dans l'ADN du groupe Orange. Et Orange Cyberdefense déploie cette connaissance pour répondre au mieux à ces enjeux de cybersécurité dans la sphère publique. Alors, au risque de choquer certains d'entre vous, pourquoi est-ce que NIS2 est une opportunité, pas une énième contrainte, une surtransposition, comme cela a été évoqué ? En tant qu'opérateur télécom dans 30 pays, avec des réseaux, des systèmes informatiques, des data centers, des câbles sous-marins, beaucoup de clients - Orange Cyber Défense a près de 10.000 grands clients dans le monde - je peux témoigner, sans même parler des JO, de l'état de la menace qui est permanente, croissante, complexe, que cela vienne de l'Est de l'Europe, d'un grand pays asiatique ou d'Amérique du Nord, parce que dans le numérique, nous n'avons pas d'amis, pas d'alliés. Imaginez seulement une seconde les tentatives de vol de brevets dont peut faire face le groupe Airbus, par exemple, face à ses concurrents. Le numérique est fantastique, il offre des bénéfices incroyables, mais il y a le revers de la médaille et le job d'Orange Cyberdéfense est d'accompagner ses clients publics comme privés dans ce chemin-là.

Il y a un autre point qui a été évoqué et sur lequel je voudrais insister. C'est que, et je peux prendre l'exemple du groupe Orange si vous le souhaitez, la cybersécurité ne doit plus être qu'un sujet de spécialistes. C'est un sujet collectif. C'est un sujet de management, de responsabilité pour chacun d'entre nous. Et donc c'est la raison pour laquelle, et encore une fois c'est un exemple particulier qui ne se transpose pas forcément à chacun d'entre vous. Chez Orange, nous avons décidé de mettre le sujet de cybersécurité au comité exécutif, donc dans le plus haut échelon de l'organisation, et ce dès 2018. Parce que sans cybersécurité, le groupe s'arrête. Les risques sont immenses, la réputation peut être ruinée. Il y a des opérateurs télécoms, tel Vodafone au Portugal, dont l'activité s'est arrêtée à la suite d'une cyberattaque. Plus de téléphone, plus de connexion Internet. Donc, c'est vraiment une question de résilience et une question de premier ordre. Et d'ailleurs, dans les organisations publiques comme privées, le risque cyber devient dans le top trois leader sur le territoire national.

Il y a aussi l'enjeu des compétences. Comment est-ce que vous allez faire pour maintenir les compétences au sein des organisations ? Mon premier indicateur de gestion et loin devant tous les autres, ce sont les ressources humaines. Ce n'est pas le chiffre d'affaires, ce ne sont pas les commandes, ni le contentement des clients. Comment je fais pour avoir le bon nombre de personnes, aux bonnes qualifications, aux bons endroits pour répondre aux clients ? C'est un enjeu majeur. Les systèmes d'éducation ne sont pas encore complètement adaptés à cet enjeu de formation continue et avec des enjeux majeurs. Et donc, nous avons besoin d'être capables d'attirer, de retenir, de former et de payer, accessoirement, des experts dans un milieu en hypercroissance. Le marché de la cybersécurité croît de 10 % par an. Donc, il y a plein d'opportunités. Il y a plein d'acteurs comme nous. Il y a plein de clients comme vous qui recrutent des gens. C'est un marché extrêmement fluide. Chez Orange Opérateur en France, le taux d'attrition qui est le taux de départ naturel hors retraite est inférieur à 5%. Le taux d'attrition dans les métiers de la cybersécurité, c'est entre 15 et 20%. Vous pouvez perdre un cinquième de votre effectif tous les ans. Les enjeux de RH, de formation, d'attractivité, sont majeurs pour nous tous, c'est un sujet de résilience collectif, et pas uniquement pour Orange Cyberdéfense. Chez Orange, nous parlons de cybersécurité toutes les semaines au comité exécutif. Et pas uniquement parce que nous sommes opérateur télécom, mais parce que ce sont nos enjeux de numérisation et de digitalisation de l'activité qui le nécessitent. Nous avons besoin d'avoir cette connaissance et de ne plus penser que c'est juste un sujet d'expertise. C'est un sujet de management et un sujet politique, comme cela a été évoqué précédemment.

Mikaël AUDEGOND

Je vous rejoins aussi sur la question de l' Éducation nationale et de peut-être définir un périmètre d'une science informatique, comme nous l'avons fait de la science physique. Cela pourrait être effectivement une piste de réflexion pour faire une première formation initiale de nos plus jeunes citoyens. L'Éducation nationale a mis en place différentes certifications, mais qui n'ont pas encore, pour des raisons de moyens, toute leur portée et toute leur dimension.

Stéphane VANGHELUWE, les opérateurs publics de services numériques, les OPSN, regroupés dans Déclic comme SITIV, accompagnent quotidiennement la transformation numérique des services publics locaux, collectivités, mais aussi régies et hôpitaux. Beaucoup d'acteurs locaux ne connaissent pas encore exactement ni les risques qu'ils encourent, ni les obligations ou les

solutions qu'il leur faudra mettre en œuvre face à ces défis de cyber. Pouvez-vous nous présenter votre approche dans la mise en place de ces mesures sur le terrain ? Comment nos territoires doivent-ils s'organiser pour y répondre ?

Stéphane VANGHELUWE

Nous sommes vraiment là en tant qu'OPSN pour répondre à ces questions que vous nous avez posées dans la salle. Comment organiser les compétences, les recruter, les maintenir ? Comment assurer la souveraineté et assurer la maîtrise des enjeux publics ? Comment financer ? Comment mutualiser ? Je fais un petit aparté : dans la dernière loi de finances, il semblerait que la récupération de la TVA sur le service SaaS pourrait être rabotée. Vous en parliez tout à l'heure. Il y a deux ans, les logiciels ne pouvaient plus être soumis à la récupération de TVA. Cette année, ils sont enlevés aussi sur le SaaS et aussi pour les produits cyber en SaaS. Raison de plus, peut-être, pour continuer à les maîtriser nous-mêmes et donc les maîtriser nous-mêmes à travers des ESN.

Je représente donc aujourd'hui deux structures. Le SITIV qui opère en région lyonnaise, environ 35.000 collaborateurs. Dans les adhérents, une population importante puisque la ville de Lyon et la métropole de Lyon font partie des membres de l'entente que nous avons montée, mais aussi Déclic, qui a hier signé une convention avec l'Avicca, parce que nous sommes bien conscients que câbles, usage, cybersécurité, fonctionnent ensemble. Et donc, nous vous invitons à nous rejoindre. Je me suis permis de repartir de la dernière étude cybermalveillance publiée la semaine dernière. Et peut-être, pour ne pas vous citer tous les chiffres, appuyer sur la forme d'inconscience des élus face au risque. Vous êtes nombreux, visiblement, à ne pas vous sentir concernés, principalement dans les communes les plus petites. C'est peut-être là d'ailleurs où Déclic a le plus gros impact. Tout à l'heure, nous parlions de 90% des communes non soumises à NIS2. C'est quand même 90% des communes soumises au risque cyber et dont 50% sont membres de structures, membres de Déclic. Donc, je vais appuyer comme vous sur la gouvernance. Messieurs les élus, aidez-nous une fois par an, une demi-heure, à regarder ce que vos équipes, vos agents, vos structures de mutualisation font. Elles vous demandent un tout petit peu de moyens, elles vous demandent des moyens humains, mais elles vous demandent surtout de les accompagner pour aller dans le bon sens tous ensemble. Qu'est-ce que c'est qu'un OPSN ? Un OPSN, c'est une structure publique, parapublique, associative. C'est un terme qui a été inventé par nous, opérateurs publics de services numériques, pour ne pas dire ESN, donc structure dont le métier est de mettre à disposition des services numériques. Et un service numérique, c'est forcément un service numérique pour les collectivités de qualité, c'est-à-dire sécurisée. Cela veut dire que nous

avons naturellement pris le sujet avec l'ANSSI. Notre mission numéro une, la plus dure, c'est de vous accompagner, de vous sensibiliser, de vous entraîner avec nous dans la démarche numérique générale. Et la cyber est le nouveau sujet. L'enjeu du dernier kilomètre. Nous avons plein d'outils, qui sont performants, qui ne sont éventuellement pas trop chers. Encore faut-il que vous les utilisiez. C'est bien l'enjeu le plus difficile et c'est un de nos rôles les plus compliqués.

Ensuite, il convient d'assurer la souveraineté, la résilience, l'interopérabilité. Un point important, donc, organiser la gouvernance. NIS2, c'est plein de mesures techniques complexes que vous allez laisser gérer par vos équipes. Vous allez leur faire confiance comme d'habitude. Mais c'est une gouvernance avec une politique de sécurité informatique, avec une perspective d'investissement, avec des audits, des procédures, des indicateurs, des suivis de projets, des tableaux de bord. Cela, messieurs les élus, vous savez faire. Vous faites depuis longtemps des plans communaux de sécurité. Rajoutez ce point-là dans vos enjeux. Nous sommes contents au sein de Déclic d'être là pour essayer d'être acteur du paysage national. Donc remercier l'ANSSI, la DINUM, l'ANCT et peut-être aujourd'hui tout particulièrement un projet sur lequel je pense que vous devez être attentif, le projet de « suite territoriale » à l'initiative de l'ANSSI, piloté par l'ANCT avec l'aide de la DINUM, pour mettre des outils de sécurité auprès des collectivités les plus petites. Vous avez, une identité numérique : avoir une adresse gmail, et pouvoir communiquer avec l'État en étant sûr que je suis monsieur le maire et que je ne me fais pas usurper mon identité par quelqu'un de l'opposition, par exemple, une messagerie sécurisée, un espace de stockage sécurisé. Ce sujet-là est un enjeu d'importance que je vous engage à regarder de près.

Nous attendions depuis très longtemps l'identité numérique des agents des collectivités locales. Vous aviez dû entendre parler d'AgentsConnect. Cela se met en route. L'État met aussi des moyens financiers et techniques à disposition des collectivités locales en l'occurrence. Qu'est-ce que c'est qu'un OPSN ? C'est une offre de services qui sont réalisés en propre ou achetés, revendus. Le maître mot, c'est qu'ils sont mis à disposition de façon centralisée, accompagnée, financée, mutualisée, optimisée, et avec 2.000 agents de terrain spécialistes du numérique en France, capables de les accompagner. Nous sommes sur presque tout le territoire, il y a quelques zones blanches, en particulier dans l'Est de la France. Nous représentons un peu plus de 50% des communes françaises. Nous avons des structures publiques de toutes sortes, des syndicats intercommunaux, des SMO, de plus en plus d'opérateurs de DSP nous rejoignent, des ATD, des GIP, des associations : 72 aujourd'hui. Le sujet de la cybersécurité est le sujet numéro un mis dans les feuilles de route de l'ensemble de nos structures. Nous avons déjà mis en route un

certain nombre d'actions en dehors des actions de collaboration avec l'ANSSI et les autres services de l'État. Au niveau national, nous sommes à l'initiative de la mise à jour et de la tenue de cette carte des attaques contre les collectivités locales et les établissements publics. Mais nous cherchons aussi à mettre en place un certain nombre d'outils mutualisés entre nous. Nous essayons d'être les chantres de la supramutualisation et donc d'être capables de partager entre une bonne initiative de la Vendée et la mettre à disposition du nord de la France. Il y en a une bonne trentaine au total qui ont été développées, mises en œuvre, entre autres pour travailler sur la cybersécurité.

Mikaël AUDEGOND

Au-delà des collectivités, quelles sont les obligations de nos délégataires sur les RIP dans le contexte de NIS2 ?

François DÉGEZ

Ma vision est peut-être un petit peu caricatural. Par rapport à tous les services que proposent les collectivités, il y a ceux qu'elles opèrent en propre. Ainsi pour une régie communale des eaux qui fait partie de la commune, c'est le système d'information de la commune qui est considéré et nous revenons donc à la situation précédente. C'est la totalité du système d'information qui est concerné. En revanche dès lors qu'une collectivité délègue par le biais d'un contrat une mission à une entité privée ou autre, c'est un contrat. Dans le cas de NIS2, il faut bien faire attention à la gestion contractuelle vis-à-vis de vos délégataires. Donc si le délégataire est de toute façon concerné, au travers de ses obligations contractuelles, il pourra l'être aussi en tant qu'entité NIS2 en fonction de sa taille et de son niveau d'activité

Mikaël AUDEGOND

Comment trouver des mécanismes pour budgéter des actions d'investissement et fonctionnement ?

Damien MICHALLET

Il y a plusieurs réalités qu'il faut avoir en tête. D'abord, NIS2, c'est une réelle opportunité, indispensable pour les entreprises privées mais une réelle opportunité aussi pour les collectivités.

C'est une vraie occasion de structurer plein de choses. Après il faut financer. Il y a d'abord un choix réel qui est un choix politique, et NIS2 est la meilleure des excuses pour sensibiliser aussi nos bureaux, nos exécutifs, quant aux axes à porter et à l'attention à porter. Ensuite, sur les financements, il y a une réalité que nous avons mise en avant dans le rapport de NIS2. C'est qu'il faut absolument faire un focus sur les plus fragiles. Tout le monde n'a pas les mêmes moyens, les mêmes organisations et la même histoire. Il est donc absolument indispensable, et peut-être en travaillant avec l'ANSSI sur ces sujets-là, non pas de financer mais d'identifier les plus fragiles et de mettre en place un fonds pour les accompagner. Sur le financement descendant, je n'ai pas toutes les réponses. Les débats s'ouvrent la semaine prochaine sur les sujets numériques, tant sur la partie infra que sur les autres sujets. Nous avons pas mal d'amendements au Sénat qui sont là pour limiter la casse plus que pour créer des opportunités.

Mikaël AUDEGOND

Quel est le rôle des CSiRT régionaux avec l'évolution NIS2 ?

François DÉGEZ

Les CSIRT, c'est une opportunité qui est née du plan France Relance. A l'origine, un certain nombre d'expérimentations avaient été menées en PACA et puis en Aquitaine, avec l'idée que très clairement, entre Cybermalveillance, qui faisait une réponse de premier niveau, mais qui n'était qu'une plateforme, et le Cert-FR, qui s'occupait des entités vraiment très critiques, au niveau intermédiaire il y avait une immense faille pour toutes les associations, collectivités, entreprises de taille intermédiaire qui se retrouvaient un petit peu seules, uniquement avec leurs prestataires. Donc, cela a été l'opportunité de proposer aux régions qui ont en charge le développement économique de monter ces CSIRT partant du principe qu'il n'y a plus de développement économique sans outils numériques, et qu'un outil numérique doit fonctionner et être fiable. Cela semblait logique de proposer aux régions de se lancer dans l'aventure et pour l'essentiel, elles ont toutes répondu présentes. Mais l'idée, c'était bien d'avoir un service de remédiation de premier niveau. Alors l'ambiguïté de ce sujet-là, c'est que nous avons dit que c'était d'abord pour répondre à un intérêt immédiat qui était d'assister les victimes lorsqu'elles étaient en difficulté et que ce service-là devait être gratuit. Mais il faut quand même que la structure fonctionne. Donc, nous avons admis qu'autour du service de remédiation, puisse être agrégés des services de sensibilisation, de formation… Cela pourrait servir à financer aussi les activités au-delà de la simple mécanique de la subvention. Pour l'instant, nous sommes dans le cadre de cette vision

qui est purement une vision remédiation. Sur le plan purement remédiation aux incidents, ce que nous avons demandé aux CSIRT, c'était de s'inscrire au réseau Inter-cert, qui est un réseau de partage d'informations techniques, de manière à ce que le l'action collective du réseau soit plus efficace. Nous savons cependant qu'il y a un vrai sujet de pérennité des financements. L'ANSSI est une autorité technique et n'a pas forcement d'avis là-dessus. La conviction que nous pouvons avoir, et ce sont les échanges que nous avons au plus haut niveau avec la DINUM, c'est qu'il ne faut pas séparer les choses entre le développement du numérique et la cybersécurité. Le développement numérique doit être sécurisé. Et donc, tout ce qui fait partie de l'accompagnement cyber doit rentrer de manière naturelle dans un pot beaucoup plus large, beaucoup plus commun de l'accompagnement global des collectivités. Certaines régions ont pu accompagner le développement des CSIRT en les intégrant dans le CPER. Mais je ne sais pas si c'est la seule solution.

Mikaël AUDEGOND

C'est peut-être un levier. Je vais remercier une dernière fois nos quatre intervenants et je pense que nous allons pouvoir les applaudir pour leur intervention et pour leur présence ce matin.