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 5 juin 2025
Séance de 11 heures 30

Compte rendu n° 9

SESSION ORDINAIRE DE **2024 - 2025**

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 11 heures 40

La commission spéciale a organisé une table ronde réunissant le Mouvement des entreprises de France (Medef) et Confédération des petites et moyennes entreprises (CPME).

M. le président Philippe Latombe. Nous poursuivons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité avec une table ronde réunissant le Mouvement des entreprises de France (Medef) et la Confédération des petites et moyennes entreprises (CPME). Le Medef est représenté par Mme Rouilloux-Sicre, vice-présidente du groupe Thalès, présidente du comité régulation du numérique, Mme Briard, chargée de mission économie numérique, et Mme David, chargée de mission affaires publiques. Au titre de la CPME, nous accueillons M. Bataille, membre du comité exécutif de la CPME en charge du numérique et de l'innovation, M. Bothorel, référent cybersécurité, Mme Bouchet, juriste commerce et consommation et M. Dufour, responsable affaires publiques.

Une enquête menée en juin 2024 par l'Agence nationale de la sécurité des systèmes d'information (Anssi) auprès des membres du Clusif et mentionnée par nos collègues sénateurs dans leur rapport sur le projet de loi révèle qu'une cyberattaque coûte en moyenne 466 000 euros pour les très petites, petites et moyennes entreprises (TPE-PME), 13 millions d'euros pour les entreprises de taille intermédiaire (ETI) et 135 millions d'euros pour les grandes entreprises.

Une autre étude menée l'année dernière auprès de 500 TPE-PME pour le compte de cybermalveillance.gouv.fr sur leur niveau de maturité en matière de risque cyber montre que la situation est alarmante. Il en ressort que 61 % des entreprises françaises de moins de 250 salariés s'estiment faiblement protégées en matière de cybersécurité ou ne savent pas évaluer leur niveau de protection. Parmi les obstacles mentionnés pour atteindre le bon niveau de cybersécurité, la moitié des entreprises invoquent le manque de temps, le manque de connaissances et d'expertise, le manque de budget ou affirment encore ne pas savoir vers qui se tourner.

L'adoption de la directive NIS 2 et sa transposition par le titre II du projet de loi que la commission spéciale est chargée d'examiner constituent des réponses à l'augmentation de la cybercriminalité. Le projet de loi distingue deux catégories d'entités régulées, les entités essentielles et les entités importantes. Cette catégorisation s'établit selon leur degré de criticité, leur taille et leur chiffre d'affaires. Selon l'Anssi, près de 2 000 entreprises privées devraient être considérées comme des entités essentielles.

Dans ce contexte, nous souhaitons vous entendre sur la manière dont vous percevez le projet de loi et sur les éventuels angles morts auxquels il faudrait remédier dans le cadre de l'examen du projet de loi par l'Assemblée nationale.

Mme Juliette Rouilloux-Sicre, vice-présidente du groupe Thales, présidente du comité régulation du numérique du Medef. Le Medef souhaite réaffirmer que ce texte, qui permet globalement d'élever le niveau de cybersécurité des entreprises françaises, est pertinent ; nous le soutenons. Les efforts de pédagogie conduits depuis maintenant un certain

temps n’ont malheureusement pas suffi, face à la multiplication des attaques, notamment celles visant les PME-ETI.

Pour autant, le Medef est très attentif à éviter une surtransposition, pour plusieurs raisons. D’abord, la directive prévoit déjà un certain nombre d’obligations qui nous semblent suffire pour élever ce niveau de cybersécurité. Ensuite, il est important d’établir une harmonisation au niveau européen. Malheureusement, NIS 2 est une directive et non un règlement. Certains pays sont un peu plus en avance que la France dans leur transposition. Pour les entreprises implantées dans plusieurs pays européens ou celles qui visent des marchés européens, il est important de pouvoir disposer d’une certaine harmonisation des pratiques.

Il est également essentiel pour les entreprises de pouvoir disposer du texte définitif de transposition dans un délai raisonnable, qui permette également un travail parlementaire de qualité. Nous souhaitons également mentionner quelques points d’attention plus particuliers, notamment l’harmonisation des définitions. En effet, le texte en droit français n’adopte pas forcément la définition de la directive, ce qui est un peu regrettable.

Ensuite, les entreprises représentées par le Medef s’interrogent sur le champ d’application couvert par la notion « d’entités », qui suscite un certain nombre d’inquiétudes. En outre, les sanctions, très significatives, soulèvent également des craintes chez nos membres. Le Medef reconnaît la pertinence des sanctions, mais souligne leur nécessaire proportionnalité. Le texte doit également préciser que ces sanctions n’interviendront qu’en dernier recours. De plus, la sanction pénale du dirigeant ne nous semble pas forcément nécessaire, puisque les dirigeants d’entreprises agissent de la meilleure manière possible et qu’ils ne disposent pas forcément d’une grande expertise dans ce domaine.

M. Franck Bataille, membre du comité exécutif de la CPME, en charge du numérique et de l’innovation. La CPME représente plus de 243 000 entreprises et 5,5 millions de salariés. Le sujet qui nous réunit aujourd’hui engage l’avenir, la compétitivité et la sécurité de notre tissu économique. Membre du comité exécutif de la CPME en charge du numérique et de l’innovation, je dirige une petite entreprise de services numériques de dix personnes dans le Loir-et-Cher. À ce titre, je connais bien la difficulté de la conformité en matière de cybersécurité pour des petites entreprises.

Je souhaite évoquer tout particulièrement le soutien aux objectifs de la loi et la responsabilité partagée. Nous souscrivons pleinement à l’ambition de rehausser le niveau de cybersécurité, tant pour protéger les entreprises que pour renforcer la résilience de notre pays. Nos adhérents sont conscients de la gravité croissante des menaces et souhaitent s’inscrire dans cette démarche.

Ensuite, je tiens à insister sur l’importance de la proportionnalité et de la non-surtransposition. Les travaux ont été menés dans un esprit d’équilibre et nous sommes satisfaits de ce point de vue, mais nous pointons l’attention sur la nécessaire progressivité, dans la mesure où toutes les structures n’ont pas forcément les mêmes moyens de mener à bien l’ensemble des actions, du jour au lendemain.

Les TPE et PME sont des entreprises pragmatiques, au contact de la réalité de l’économie de terrain. Un certain nombre d’exigences pèsent déjà sur elles et nous ne voudrions pas qu’elles fassent l’objet d’obligations et de contrôles ressentis comme

disproportionnés et difficilement applicables d'une seule traite. Nous insistons donc sur la nécessité de leur accorder du temps et de les traiter de manière proportionnée.

Dans ces conditions, nous souhaitons travailler sur les éléments d'accompagnement, de pédagogie et de soutien opérationnel. Nous voulons avancer main dans la main avec vous, dans un esprit de confiance, de dialogue et de coconstruction. Nous soutiendrons les démarches qui favoriseront l'information, l'accompagnement, la proportionnalité, la tolérance, afin que la cybersécurité devienne un réflexe partagé, accessible à tous, mais également une source de compétitivité pour nos PME.

Mme Anne Le Hénanff, rapporteure. S'agissant des sanctions pénales du dirigeant, je tiens à rappeler que dans le cadre du règlement général sur la protection des données (RGPD) et de la fuite manifeste de données, la sanction pénale intervient s'il existe une preuve manifeste de non-volonté de se mettre en conformité. Il me semble que la directive NIS 2 partage le même esprit, mais nous pourrons en reparler si vous estimez que des précisions doivent être apportées dans le texte.

Que pensez-vous de l'idée, promue par certains acteurs, de rendre visible la démarche, voire l'atteinte, de la conformité à NIS 2 ? Que pensez-vous de l'idée d'une labellisation ?

Ensuite, j'aimerais connaître votre analyse sur les contrôles et les audits. Cet aspect suscite fréquemment des réactions, notamment de la part de ceux qui questionnent l'indépendance des organisations qui pourraient effectuer ces contrôles, voire qui souhaiteraient que celles-ci soient exclusivement françaises ou européennes. L'audit doit-il être généré par l'autorité de contrôle, l'Anssi, ou par l'entité elle-même concernée ? Comment appréhendez-vous cette thématique ?

Enfin, comment intégrez-vous la mise en conformité des 15 000 entités soumises à la directive NIS 2 vis-à-vis de leurs fournisseurs ou partenaires ? Estimez-vous que le contrat sera rempli lorsque les 15 000 entités se seront mises en conformité ou allez-vous plus loin, notamment vis-à-vis de la chaîne d'approvisionnement, en amont ou en aval ?

M. le président Philippe Latombe. Je partage les questions de Mme la rapporteure sur la labellisation et ses propos sur la sanction de l'intentionnalité. Certaines personnes qui ont été auditionnées promeuvent l'idée de la création d'un référent cyber au sein des entreprises, en mesure de s'adresser directement à l'organe dirigeant en cas de difficultés. Quel est votre point de vue à ce sujet, à la fois dans les grandes entreprises, mais aussi dans les PME et TPE ?

Ensuite, beaucoup souhaitent que le texte de loi fasse référence à des normes internationales existantes du type ISO 27000. Qu'en pensez-vous ? L'Anssi y est plutôt défavorable, mais d'autres pays ont opéré ce choix dans la transposition, notamment la Belgique.

Enfin, certaines personnes auditionnées pointent qu'un délai de notification d'une journée est trop court, car il est nécessaire de mener des investigations. Ils souhaiteraient pouvoir modifier ou moduler ce délai, avoir la capacité de pouvoir revenir sur des déclarations d'incidents ; lorsqu'ils sont moins graves qu'initialement redoutés, ou inversement. Comment envisagez-vous ce délai de notification ?

M. Marc Bothorel, référent cybersécurité, CPME. Tant que le règlement européen sur la cyber-résilience (Cyber Resilience Act, CRA) n'aura pas été mis en application par les différents fournisseurs et que les entreprises n'auront pas la possibilité de choisir un logiciel conforme au CRA, il apparaît difficile de sanctionner un chef d'entreprise qui se ferait attaquer au travers d'une chaîne logicielle.

Certaines PME sont directement assujetties à NIS 2, mais il leur faudra s'assurer que leurs sous-traitants proposent le même niveau de sécurité, même s'ils ne sont pas eux-mêmes assujettis. Dans le texte initial fourni par l'Anssi sur les vingt règles à mettre en œuvre et les entités capables de vérifier la mise en œuvre de ces mesures, figurent essentiellement des labellisés Anssi. Ils sont pourtant trop peu nombreux pour pouvoir traiter la masse des nouvelles sociétés qui seront soumises à cette réglementation.

Nous suggérons donc de s'appuyer sur les labellisés ExpertCyber, actuellement au nombre de 200 sur le territoire. Ces experts sont spécifiquement labellisés par l'Association française de normalisation (Afnor) pour traiter les TPE-PME. Ce label pourrait évoluer avec un volet spécifique dédié à la directive NIS 2, afin de vérifier la conformité à cette dernière des entités, des assujettis et donc de nos adhérents.

Pour l'aspect relatif aux sanctions, il faut considérer que certaines chaînes logicielles ne sont pas encore conformes au règlement européen sur la cyber-résilience, tant qu'il n'aura pas été mis en application. Ensuite, le sujet du référent NIS 2 est effectivement une bonne question. Cependant, sa mise en place semble compliquée. Dans les petites entreprises, le dirigeant pourrait assumer ce rôle, éventuellement aidé par un cabinet juridique.

M. Franck Bataille. Il y a trente ans, dans les TPE-PME, le point de contact sur les technologies de l'information était le comptable. Désormais, il s'agit du dirigeant. Obliger ces petites structures à disposer d'une personne spécifiquement formée à ces enjeux pourrait entraîner des coûts supplémentaires de recours à un prestataire externe, similaires à ceux engendrés par les délégués à la protection des données (DPO). Pour le niveau attendu du point de contact, tout dépendra des besoins de chaque entreprise, en fonction de sa taille. Une TPE de cinq personnes ne peut pas être tenue aux mêmes exigences qu'une PME de 200 personnes.

M. Marc Bothorel. Nous travaillons depuis deux ans, maintenant, avec l'Afnor sur une « Spec Afnor, dont l'objectif consiste à protéger les TPE-PME de 80 % des attaques les plus communes. Cette Spec est quasiment terminée et nous avons établi un groupe de travail, qui réunit notamment la direction générale des entreprises (DGE), l'Anssi, cybermalveillance.gouv.fr, les syndicats patronaux, les syndicats IT, BoostAeroSpace et La Poste. Cette Spec est rédigée et il ne nous reste plus qu'à traiter la labellisation des entreprises capables de vérifier sa conformité. J'ai d'ailleurs transmis le dossier à Clara Chappaz, la ministre déléguée chargée de l'intelligence artificielle et du numérique, et à l'Anssi. Nous estimons que la Spec Afnor peut être utile pour les sous-traitants, dans la mesure où elle comporte plusieurs niveaux (Silver, Gold et Platinum) et fournit un cadre de référence qui n'existe pas aujourd'hui.

Ensuite, une question a été posée concernant les délais de notification d'incidents. Un délai d'un jour paraît extrêmement court. Proposer un délai de soixante-douze heures, aligné sur les fuites de données pour la Commission nationale de l'informatique et des libertés (Cnil), pourrait être cohérent, car les incidents cyber et les fuites de données sont souvent concomitants.

Mme Anne Le Hénanff, rapporteure. Je me permets de vous rappeler que deux autres questions portent sur les organismes de contrôle nationaux et européens et sur l'affichage public de la mise en conformité.

M. Marc Bothorel. Une des missions d'un syndicat patronal consiste à diffuser l'information auprès des adhérents et les inciter à se mettre en conformité. À ce sujet, l'Anssi compte sur nous. Il ne faut pas rééditer la même erreur que pour le RGPD et ne parler de la directive NIS 2 que sous l'aspect des sanctions, mais bien valoriser la conformité comme un atout commercial, celui d'être considéré comme un « partenaire de confiance ».

Mme Juliette Rouilloux-Sicre. La rédaction actuelle sur les sanctions mérite sans doute d'être affinée, pour correspondre à l'état d'esprit qu'évoquait Mme la rapporteure.

Le label de conformité doit être bien encadré pour éviter des autodéclarations subjectives. Un vrai cahier des charges est donc nécessaire, en laissant du temps aux entreprises pour se mettre en conformité. En effet, le degré de maturité cyber n'est pas le même selon la taille de l'entreprise. Dans ce cadre, l'Anssi semble désignée pour octroyer ce label en tant qu'entité de confiance, mais sera sans doute confrontée à une problématique de moyens. Quoi qu'il en soit, le label permettrait à tous, y compris aux citoyens, de connaître le niveau de conformité.

La conformité doit aussi être envisagée comme une opportunité de développement des affaires : le Medef considère qu'une entreprise responsable s'orientera plus naturellement vers un prestataire conforme.

Nous comprenons la logique des contrôles et des audits. Les contrôles, internes ou externes, sont essentiels, mais il convient de veiller à ce que les prestataires qui offriront des services soient bien compétents. Le Medef ne voit aucun obstacle à des contrôles effectués par l'Anssi, mais fait preuve de vigilance sur d'éventuels conflits d'intérêts si des tiers interviennent. Dans quelles conditions agiront-ils ? Quels seront les critères de sélection ? En effet, un auditeur pénètre au cœur des systèmes et peut accéder potentiellement à un certain nombre de failles. La même vigilance concerne les éléments de souveraineté.

Ensuite, dans le cadre de la directive NIS 1, il est parfois difficile pour les entreprises de transférer leurs exigences aux fournisseurs et prestataires. En revanche, nous estimons que NIS 2 peut offrir une opportunité, dans la mesure où elle concernera un bien plus grand nombre d'entreprises. De fait, la prise de conscience des entreprises sur la cybersécurité sera rehaussée avec cette réglementation. Pour autant, la démarche sera complexe, raison pour laquelle nous sommes vigilants en termes de surtransposition : il ne faudrait pas imposer à des fournisseurs sous-traitants de taille plus modeste des exigences qu'ils ne pourraient pas tenir.

À ce titre, il faut veiller à établir une harmonisation au niveau européen, dans la mesure où les fournisseurs et sous-traitants français ne travaillent pas toujours uniquement avec des entreprises françaises. Je pense notamment aux ETI ou aux PME, qui ont moins de moyens, moins de capacités à se mettre en conformité.

Ensuite, le rôle de référent cyber nous semble effectivement constituer une bonne idée, mais il ne devrait pas nécessairement être tenu par le responsable de la sécurité des systèmes d'information (RSSI), qui pourrait être considéré comme juge et partie. Dans la mesure où il s'agit d'un sujet de conformité, cette tâche pourrait être assurée par le directeur juridique. Le Medef recommande depuis longtemps une montée en compétences sur ces sujets

cyber, pour l'ensemble du tissu industriel français. À cet égard, des efforts de formation devraient être accomplis, mais à moindre échelle, puisque la cybersécurité est désormais mieux connue.

Utiliser des normes internationales comme ISO ou celles en cours de développement par l'Afnor est bénéfique, mais il est crucial que ces normes s'appliquent uniformément à tous. En effet, la directive NIS 2 implique une responsabilité qu'il ne faut pas restreindre uniquement aux grandes entreprises, au risque de créer des « trous dans la raquette ». Je rappelle ainsi que l'objectif initial de la directive consistait bien à s'assurer d'un bon niveau de cybersécurité en Europe. Ceci est d'autant plus important que les attaques sont aujourd'hui très variées ; elles touchent tous les secteurs d'activité et toutes les tailles d'entreprise.

Vous avez également mentionné les délais de notification. À ce titre, il convient de distinguer les fuites de données personnelles, qui font l'objet de déclarations à la Cnil, et les fuites de données industrielles. Dès lors, il n'est pas forcément pertinent d'intégrer dans le texte une déclaration d'office à la Cnil en cas d'incident cyber au titre de NIS 2, puisqu'un incident cyber ne donne pas forcément lieu, heureusement, à une fuite de données personnelles.

Le délai de vingt-quatre heures ne pose pas de problème au Medef, dès lors qu'il concerne une première notification. En revanche, il importe sans doute d'apporter une clarification concernant le type d'incident de cybersécurité qu'il convient de déclarer, dans la mesure où plusieurs dizaines de milliers d'incidents cyber interviennent chaque jour. Nous relevons avec satisfaction que la nouvelle version du texte apporte d'ailleurs une amélioration en ce sens. À l'inverse, un délai de soixante-douze heures peut sembler long : de nombreuses données peuvent avoir fui, des systèmes être bloqués. En conséquence, il peut être très utile pour une ETI d'obtenir le soutien de l'Anssi dans un délai plus rapide.

Nous sommes en revanche favorables à l'établissement d'un formulaire unique et, idéalement, d'un guichet unique, qui pourrait être assuré par l'Anssi, laquelle pourrait coordonner les déclarations et assurer la conformité. Or la rédaction actuelle du texte ne prévoit pas cette possibilité.

Enfin, je souligne que diverses autorités sectorielles mettent également en place des dispositifs en matière de cybersécurité.

M. Marc Bothorel. NIS 2 formule des exigences en matière de formation des utilisateurs. Aujourd'hui, nos adhérents cotisent aux fonds professionnels, les opérateurs de compétences (Opco) tous les mois de février, mais ne dépensent pas nécessairement leur budget. S'il ne s'agit pas d'une formation certifiante, elle constitue malgré tout la première ligne de défense d'une entreprise et désormais une exigence des assurances cyber. Ne serait-il pas envisageable de prendre en charge ces sensibilisations annuelles dans le cadre des Opco ? Compte tenu du contexte économique et géopolitique, cela mettrait le pied à l'étrier à des chefs d'entreprise pour la formation de leurs employés, de manière annuelle.

S'agissant des autorités de contrôle, vous avez évoqué ISO 27001. Cependant, pour une PME de cinquante personnes, le coût d'une conformité ISO 27001 est hors de portée. À ce propos, je me permets de rappeler une décision du tribunal d'appel de Rennes, qui a condamné un sous-traitant pour manquement à son devoir de conseil auprès d'une entreprise qui a subi une cyberattaque. Cette décision fera vraisemblablement jurisprudence. De fait, les

prestataires IT ont tout intérêt à effectuer leur métier de la manière la plus rigoureuse, dans le cadre de NIS 2.

M. le président Philippe Latombe. La directive NIS 2 prévoit que l'Anssi élabore un référentiel qui ne figure pas dans le texte de loi, mais prendra la forme d'un décret en Conseil d'État. Cela vous pose-t-il un problème d'instabilité juridique, de visibilité et de prévisibilité ?

De leur côté, un certain nombre de pays européens ayant déjà transposé ont pleinement utilisé les considérants de la directive, en estimant qu'il fallait le plus possible faire référence à des normes internationales, de type ISO 27001. Les législateurs belges ont ainsi inscrit dans le texte de loi une référence directe à de telles normes internationales. Faut-il en faire autant où maintenir une forme de souplesse, ainsi que l'Anssi le suggère ?

Mme Juliette Rouilloux-Sicre. Certains pays ont inclus des termes comme « *notamment* » ou « *de type* », créant ainsi de l'insécurité juridique. Le Medef n'est pas opposé à une définition du référentiel après la promulgation de la loi, tant que cela ne prend pas trop de temps. La transposition de la directive en droit français a pris plus de temps que prévu, même si cela permet de conduire des consultations, comme celle à laquelle vous nous permettez de participer. Cependant, le texte prévoit de nombreux renvois à des décrets en Conseil d'État, s'agissant notamment du référentiel. Or nous redoutons que ces décrets tardent à être publiés, d'autant plus que l'Anssi dispose de ressources limitées. Par ailleurs, il n'y a pas de délai de mise en conformité : en théorie, les entreprises devront être conformes immédiatement, d'un strict point de vue juridique.

Nous recommandons que le référentiel soit rapidement établi et qu'il ne s'éloigne pas trop des standards internationaux. Nous sommes préoccupés par la façon dont les entreprises choisiront leurs prestataires sans critères clairs. Il est important que la mise en place du référentiel prenne en compte les spécificités françaises tout en restant alignée avec les normes internationales.

M. Franck Bataille. Nous ne sommes pas non plus pas opposés à une définition du référentiel après la promulgation de la loi, sous réserve qu'elle intervienne rapidement. Il ne faudrait pas non plus qu'il soit inapplicable pour les TPE et PME. En effet, un référentiel trop pointu ne pourrait pas être mis en œuvre par ces dernières. Il faut tenir compte des réalités de terrain. À titre d'exemple, dans mon petit département du Loir-et-Cher, 80 % de mes adhérents ont encore une adresse wanadoo.fr. Il sera très compliqué de leur faire sauter plusieurs marches du jour au lendemain. Nous plaidons donc en faveur d'une démarche progressive dans le cadre d'un référentiel, qui doit être appliqué différemment en fonction de la dimension des entreprises.

M. Marc Bothorel. Je complète ces propos concernant la déclaration de l'incident. En tant que réserviste à l'Unité nationale cyber, je souhaite mettre en lumière une problématique sur laquelle nous avons travaillé. Certaines petites entreprises ont tenté de faire des demandes auprès de l'Anssi, bien que ce ne soit pas son rôle pour des sociétés d'environ cinquante personnes : elle traite principalement d'acteurs de plus grande taille, appelés opérateurs de services essentiels (OSE) et opérateurs d'importance vitale (OIV), dans l'ancienne nomenclature.

Il est donc pertinent de souligner l'importance du numéro 17Cyber, qui a été créé pour fournir une permanence gendarmerie-police, vingt-quatre heures sur vingt-quatre et sept

jours sur sept, capable d'aider les petites entreprises dans leurs déclarations d'incident. Des retours du terrain, notamment de brigades de gendarmerie, montrent que certains chefs d'entreprise n'ont pu déposer plainte faute de spécialistes présents.

Le mécanisme mis en place depuis le 17 décembre dernier constitue une solution appropriée pour les PME. Il permet à ces entreprises de bénéficier d'un support adapté pour toutes leurs déclarations d'incident, contrairement à l'Anssi qui ne traite pas les cas des PME de cette taille.

Mme Juliette Rouilloux-Sicre. L'Anssi a déjà fait circuler quelques versions de son référentiel et une nouvelle version sera bientôt disponible. Inspirés par des secteurs comme l'aéronautique, où Boost Aerospace utilise des niveaux de conformité (Silver, Gold et Platinum), nous pourrions envisager un référentiel similaire. Celui-ci tiendrait compte de la criticité des activités confiées aux sous-traitants et prestataires.

J'insiste à mon tour sur le caractère crucial des délais. Il est impératif que ce référentiel soit publié rapidement. Les entreprises ont besoin de clarté pour mettre en œuvre les directives, estimer les coûts et ajuster leurs offres en conséquence. Pour le moment, elles attendent.

Mme Anne Le Hénanff, rapporteure. Je tiens à réagir en ce qui concerne les décrets, pour partager l'opinion qui vient d'être exprimée. À titre d'exemple la loi visant à sécuriser et à réguler l'espace numérique (loi Sren) date de l'année dernière. Pourtant, sur la partie *cloud* que je portais, 80 % des décrets n'ont toujours pas été publiés. Il sera donc utile de transmettre ce message à Mme la ministre, que nous auditionnerons prochainement.

Ensuite, je souhaite vous poser deux questions concernant l'accompagnement, étant donné que vous représentez des fédérations professionnelles. Premièrement, envisagez-vous de mettre en place des campagnes ou des actions visant à sensibiliser vos membres, notamment pour éviter les effets d'aubaine des offres commerciales proposées par des cabinets profitant de textes non encore publiés ? Depuis déjà un an, certains vendent des services de mise en conformité avec NIS 2 alors même que le texte n'est pas encore sorti. Comment comptez-vous sensibiliser vos membres à ce sujet ?

Deuxièmement, envisagez-vous d'identifier activement vos ressortissants concernés par NIS 2, ou les laisserez-vous se déclarer eux-mêmes à l'Anssi ? J'aimerais comprendre comment vous intégrez ces éléments dans vos stratégies de communication.

M. Marc Bothorel. Nous avons également organisé des réunions avec l'Anssi sur ce sujet et sommes quelque peu déçus de la manière dont l'Anssi nous délègue cette responsabilité. Le dernier message reçu indiquait en substance : « *Nous n'avons pas de support de présentation à vous fournir, débrouillez-vous et faites de la publicité auprès de vos adhérents* ».

Au-delà, le seul outil disponible, « MonEspaceNIS2 », est toujours en phase bêta pour la partie relative à la qualification. Un autre point préoccupant concerne l'absence d'étude d'impact, ce qui nous empêche d'informer nos adhérents sur le temps et le coût nécessaires à la mise en conformité. Cela est extrêmement regrettable. Nous avons d'ailleurs déjà évoqué ce sujet auprès de Vincent Strubel, le directeur général de l'Anssi.

M. Franck Bataille. Pour répondre à votre question sur l'effet d'aubaine, nous avons déjà travaillé sur ce sujet, que ce soit pour NIS 2 ou pour le RGPD. Nous avons relayé des messages indiquant que les plateformes en ligne qui promettent monts et merveilles ne reflètent pas la réalité. Nous sommes également vigilants sur l'arrêt du cuivre, qui crée des opportunités pour certains, mais peut induire en erreur nos TPE et PME avec des offres non pertinentes ou viables. Nous continuons d'expliquer ces aspects à nos membres, tout comme le font les associations locales dans leurs collectivités. Nous veillons régulièrement à ce que nos unions territoriales portent également ce message.

M. Marc Bothorel. Nos adhérents ne sont pas des spécialistes. Nous attendions de l'Anssi que l'ensemble des règles techniques qui ont été édictées soient établies de manière plus compréhensible. En effet, elles s'adressent essentiellement à des directeurs des services informatiques (DSI) et des RSSI. J'ai récemment eu l'occasion d'en discuter avec le Clusif et nous partageons le même point de vue à cet égard : une approche progressive serait clairement bénéfique.

Cette progressivité doit aussi s'inscrire dans une démarche de bienveillance pendant le temps de la mise en place, en prenant en considération la situation économique et géopolitique, ainsi que les problématiques de trésorerie auxquelles les entreprises sont aujourd'hui confrontées. Le coût de mise en œuvre initiale de NIS 2, sans parler des coûts annuels récurrents, impactera fortement la trésorerie des petites entreprises. Il est donc nécessaire d'établir une période de bienveillance et d'accompagnement de la part de l'Anssi et de l'écosystème, ainsi qu'une écriture des règles à mettre en œuvre de manière progressive, à partir d'un socle sur lequel sera progressivement construit l'ensemble des règles et des obligations de NIS 2. Actuellement, les vingt règles sont posées d'un coup, et il incombe aux utilisateurs de décrypter leur contenu, ce qui n'est pas toujours simple pour un non-spécialiste.

M. le président Philippe Latombe. Nous avons souhaité, comme l'a exprimé le rapporteur général, organiser une première audition avec le directeur général de l'Anssi. Nous le réauditionnerons une dernière fois après toutes les auditions, pour revoir les points soulevés et envisager éventuellement des évolutions. Ensuite, nous auditionnerons en dernier la ministre qui portera le texte, ce qui servira de base à notre discussion générale pour la commission. À ce titre, les messages que vous nous adressez aujourd'hui sont nécessaires pour les deux auditions à venir. Les auditions publiques permettent précisément d'élargir le spectre du débat.

Mme Juliette Rouilloux-Sicre. Le Medef a pour habitude d'accompagner ses adhérents et le débat sur la cybersécurité n'y déroge pas. Une fois que le texte aura été publié, nous agirons en ce sens de manière encore plus poussée, en essayant de faire œuvre de pédagogie. À ce sujet, nous souhaiterions pouvoir disposer de documents standards, que chaque organisation pourrait diffuser de la même manière au sein de ses fédérations. Mais nous n'avons pas attendu pour agir. Une équipe numérique du Medef y travaille, y compris sous la forme de webinaires.

Le Medef croit beaucoup à la cybersécurité et estime qu'il s'agit d'un point fort en termes de souveraineté. Encore une fois, avoir des documents standardisés aiderait à assurer la bonne compréhension et à éviter les mauvaises interprétations.

Sur le sujet de l'identification des entreprises, le Medef ne prendra pas la responsabilité, car elle incombe à l'entreprise elle-même. NIS 2 prévoit d'ailleurs une charge de la preuve un peu différente par rapport à NIS 1. Les entreprises doivent s'identifier, faire

leur propre auto-évaluation et déterminer si elles sont une entité essentielle, importante ou non concernée. Nos adhérents demandent un accompagnement plus prononcé de l'Anssi sur le sujet, qui tarde pour le moment, pour des raisons que nous comprenons par ailleurs, tant elle doit couvrir un grand nombre de secteurs et d'entreprises.

Il n'en demeure pas moins que nombre d'entreprises aimeraient un accompagnement plus marqué de l'Anssi sur la qualification, pour pouvoir s'assurer qu'elles ont choisi la bonne. De fait, dans leur très grande majorité, les entreprises font preuve d'une très bonne volonté, ont envie de se mettre en conformité. Mais parfois, leur niveau de maturité cyber n'est pas encore excellent.

Je me permets également de revenir sur un point abordé lors de mon exposé liminaire. Il est important d'utiliser un vocabulaire cohérent dans le texte de transposition, afin d'éviter les différences de définition entre le droit français et la directive. Pour les groupes ayant des entités dans plusieurs pays européens, il faudrait envisager un guichet unique. En effet, contrairement au RGPD, NIS 2 manque d'un tel outil, ce qui complique la gestion des incidents pour les grandes entreprises multinationales.

La directive NIS 2 complique la tâche de deux types d'entreprises. Il s'agit d'une part des petites et moyennes entreprises, parce qu'elles ne connaissent pas très bien le cyber. Il s'agit d'autre part des grands groupes, présents dans un certain nombre de pays européens et dont les qualifications sont parfois différentes selon les pays, selon la transposition qui a été opérée en droit national. En conséquence, ils doivent notifier et se déclarer auprès de plusieurs autorités de contrôle.

En résumé, il serait opportun que le législateur français prête une attention particulière aux terminologies utilisées et que l'Anssi puisse jouer un rôle de guichet unique et fournir un support.

M. le président Philippe Latombe. Il existe effectivement une forte demande de la part des entreprises, quel que soit leur secteur. Souhaitez-vous aborder d'autres points ?

M. Marc Bothorel. Je souhaite revenir sur la nécessité d'un accompagnement budgétaire pour aider nos adhérents à se mettre en conformité dans un domaine, qui n'est pas aujourd'hui perçu comme un outil de productivité. Actuellement, nous constatons le « saupoudrage » des différents budgets accessibles, sujet que nous avons déjà abordé devant la commission sénatoriale. À cette occasion, j'avais pris l'exemple d'une petite entreprise implantée dans la « diagonale du vide » qui serait soumise à NIS 2, sans prestataire à proximité, sans faculté d'accéder à des budgets.

Il est donc essentiel d'assurer une égalité de traitement et d'accessibilité aux budgets accompagnant les PME pour se mettre en conformité.

Malheureusement, cela n'est pas le cas aujourd'hui. Dorothée Decrop, déléguée générale d'Hexatrust, que vous avez reçue un peu plus tôt ce matin, réalise un travail formidable pour essayer d'identifier les différentes sources de budgets disponibles auprès des entreprises. Mais au-delà de l'identification, l'essentiel consiste surtout à pouvoir accéder à ces budgets. Or il existe de très fortes distorsions dans ce domaine. À titre d'exemple, en Île-de-France, le budget de 10 millions d'euros mobilisé par le conseil régional pour les PME n'était accessible qu'aux entités labellisées « prestataire d'audit de la sécurité des systèmes

d'information » (Passi) par l'Anssi, dont les coûts par journée étaient trop élevés pour des budgets de PME.

Si nous voulons réussir la mise en œuvre de NIS 2, il faut introduire de la rationalité, à la fois sur la capacité de nos adhérents à accéder effectivement à des prestataires capables de les mettre en conformité, mais également à des accompagnements budgétaires pour la mise en conformité. Lorsqu'internet s'était diffusé, dans les années 2000, une loi de finances avait inscrit un crédit d'impôt de 50 % pour s'équiper en équipements réseau et ainsi accéder à internet. Ne pourrait-on pas imaginer un dispositif similaire ?

Toutes choses égales par ailleurs, un investissement de l'État pour aider les entreprises à se protéger lui coûterait moins cher que les conséquences d'attaques cyber sur celles-ci, qui se traduiraient par des dépôts de bilan, des mesures de redressement, des recettes fiscales en moins et des chômeurs supplémentaires, qu'il faudrait indemniser.

M. Franck Bataille. Dans certaines régions, comme le Loir-et-Cher, la complexité et la multiplicité des dispositifs peuvent retarder considérablement la mise en place de mesures de cybersécurité. Dans mon département, j'ai le souvenir d'un adhérent, employeur de soixante salariés qui voulait mettre en place différentes mesures de cybersécurité. Il lui a fallu plus d'un an pour aller au bout de la démarche. Il arrive qu'un plus grand nombre de ressources soient dépensées pour préparer les dossiers de demande d'aides que pour bénéficier réellement de ces aides. Simplifier et améliorer l'efficacité de ces dispositifs pourrait grandement aider les PME.

M. le président Philippe Latombe. Ce type de questions sera abordé avec Mme la ministre, même si elles relèvent plus de la loi de finances que d'un texte de cet ordre.

Ensuite, nous avons longuement évoqué aujourd'hui les sanctions de nature pénale. En revanche, je suis surpris qu'aucun de vous n'ait mentionné le fait que seules les entreprises étaient soumises à une possibilité de sanction alors que le secteur public n'est pas concerné. Quel est votre point de vue à ce sujet ?

Je souhaite enfin vous poser une question au nom notre collègue Mickaël Bouloux, rapporteur en charge de la partie relative à la directive Dora. Avez-vous identifié des zones de frottement, des incompatibilités, entre la directive NIS 2 et Dora qui justifieraient des modifications du texte de transposition, pour le rendre cohérent ? En effet, selon diverses personnes auditionnées, Dora prévoit que les entreprises assujetties à la directive puissent diligenter des audits auprès de leurs sous-traitants. Deux remarques ont été formulées à ce propos. D'une part, la durée et le coût de ces audits ne sont pas détaillés. D'autre part, cette question soulève des préoccupations concernant l'accès potentiel à des informations sensibles par des cabinets étrangers. Ce sujet vous préoccupe-t-il ? Avez-vous des recommandations à formuler à ce propos ?

Mme Juliette Rouilloux-Sicre. Pour le Medef, la disproportion un peu systématique sur ces sujets de conformité entre les entités publiques et les entreprises ne semble pas pertinente. Actuellement, le niveau de cybersécurité des collectivités est parfois bas, ce qui peut s'expliquer par différentes raisons. Elles sont soumises à d'autres types de demandes de la part des citoyens, qui ne portent pas vraiment sur le cyber, mais plutôt sur des préoccupations plus classiques comme la qualité des équipements, le bon fonctionnement des écoles.

Néanmoins, nous redoutons qu'en l'absence de sanctions, ces collectivités ne prennent pas ce sujet à bras-le-corps et ne le traitent pas avec autant diligence que les entreprises, alors même qu'elles ont accès à un certain nombre de données importantes pour le secteur privé. Les entreprises leur communiquent par exemple des données qui sont parfois sensibles. Il nous semble important que l'ensemble de l'écosystème français se mette en conformité, même s'il ne revient pas au Medef de prôner telle ou telle sanction pour les administrations ; notre organisation défend les entreprises.

En revanche, nous considérons que le montant des sanctions est extrêmement élevé et que leur assiette de calcul n'est pas complètement claire, notamment pour les groupes d'entreprises. Ces sanctions sont ainsi déterminées par rapport au chiffre d'affaires. Mais de quel chiffre d'affaires est-il question ? S'agit-il de celui de l'entité qui a commis une négligence ou de celui du groupe en entier ? Le Medef préfère évidemment la première possibilité, dans la mesure où un groupe n'est pas forcément informé de ce qui se passe dans l'une des entités. Par ailleurs, nous considérons que le montant des sanctions est effectivement très significatif ; elles peuvent mettre en péril l'activité des entreprises. Nous avons compris que la mise en œuvre serait effectuée avec une certaine bienveillance, mais le Medef est très vigilant à ce sujet.

Ensuite, vous avez mentionné les craintes liées à la conduite des audits par des cabinets étrangers. Compte tenu de la responsabilité qui pèse sur les donneurs d'ordre dans le cadre de NIS 2, il nous semble utile qu'ils puissent mener des audits auprès de leurs sous-traitants et fournisseurs. Cela permet effectivement de vérifier la conformité sur des activités critiques pour la nation et certains secteurs. En revanche, ces contrôles et audits doivent être conduits par des entreprises labellisées. Il existe déjà un certain nombre de labellisations cyber.

Le texte prévoit également la possibilité pour les autorités d'échanger avec des organismes internationaux qui œuvrent dans le domaine de la cybersécurité. En revanche, ni la directive NIS 2, ni le texte de transposition ne fournissent de détails. Le Medef souhaite s'assurer que des informations confidentielles, y compris celles liées au secret des affaires, ne soient pas transmises à des tiers dans le cadre de discussions internationales.

Enfin, en matière de normes, le Medef préfère des normes internationales établies plutôt que des normes très spécifiques et sectorielles : nous préférons une norme ISO à une norme Afnor, car elle nous semble plus correspondre à l'objectif d'harmonisation.

M. Franck Bataille. Nos territoires sont très impliqués dans le développement économique. Les relations de la CPME avec les collectivités territoriales sont extrêmement fréquentes. Nous partageons avec elles un grand nombre d'informations, parfois stratégiques. Quelle que soit la taille des entreprises, nous sommes dans une relation de confiance, notamment concernant les informations que nous leur confions. De fait, les collectivités sont très souvent les premières informées de nos projets économiques, comme la construction de bâtiments. Nous croyons en leur accompagnement, en leur bienveillance et en leur aide, et nous ne voudrions pas que les informations que nous transférons soient dispersées ou fassent l'objet de fuites. C'est la raison pour laquelle les acteurs publics devraient aussi porter, selon nous, leur part de responsabilité, de la même manière que les collectivités locales sont aujourd'hui responsables en matière de RGPD.

Ces collectivités territoriales sont des partenaires, au même titre que l'ensemble de notre chaîne d'approvisionnement, elles font aussi partie de l'écosystème. Elles partagent

également un certain retard dans l'appréhension des enjeux cyber, au même titre que les TPE et PME. Je le sais d'autant mieux que j'ai été sollicité la semaine dernière pour intervenir lors d'un congrès de maires de petites communes dans mon département, au titre d'expert cyber. Un grand travail reste à accomplir vis-à-vis de ces acteurs territoriaux, qu'il faudra aussi responsabiliser.

M. Marc Bothorel. S'agissant de la responsabilité du chef d'entreprise, nous avions déposé un amendement, qui avait été accepté, auprès de la commission sénatoriale, en faveur d'une proportionnalité en fonction de la gravité du manquement. Cette mesure vise à éviter des sanctions trop lourdes qui pourraient mettre en difficulté des entreprises.

Enfin, je souhaite vous faire part d'un exemple pour illustrer les difficultés auxquelles nous sommes confrontés pour transmettre les messages et informations. Nous avions organisé en Ardèche une réunion d'information conjointe avec la chambre de commerce, la préfecture, une importante communauté de communes, la gendarmerie et le conseil départemental au sujet de NIS 2, à destination des entreprises. Cet événement, qui devait se dérouler le 12 juin, vient d'être annulé. Seulement six personnes s'étaient inscrites.

M. le président Philippe Latombe. Je vous remercie. Nous ne savons pas encore quand ce texte sera étudié dans l'hémicycle, probablement en septembre. Dans l'intervalle, n'hésitez pas à faire parvenir des contributions écrites à nos rapporteurs, afin que nous puissions les intégrer à notre réflexion et produire un texte le plus lisible et efficace possible. L'objectif consiste en effet à éviter des zones d'ombre et des effets de bord.

La séance est levée à 13 heures.

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 5 juin 2025 à 11 h 40

Présents. - M. Philippe Latombe, Mme Anne Le Hénanff