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

Mercredi 4 juin 2025
Séance de 17 heures

Compte rendu n° 7

SESSION ORDINAIRE DE **2024 - 2025**

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 16 heures 55

La commission spéciale a organisé une table ronde réunissant des entreprises de télécommunications.

M. le président Philippe Latombe. Mes chers collègues, 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 consacrée aux entreprises de télécommunications.

Le panorama de la cybermenace 2024 de l'Agence nationale de la sécurité des systèmes d'information illustre la diversité et la gravité des menaces qui pèsent, entre autres, sur ce secteur. Sont distinguées les menaces à visée lucrative, celles à finalité d'espionnage, et enfin celles visant à déstabiliser nos sociétés, dans lesquelles s'inscrivent les actes de sabotage. Ainsi, l'ANSSI a traité en 2024 la compromission et le chiffrement par le biais d'un rançongiciel d'une entité du secteur des télécommunications. Fait marquant de 2024, certaines rares attaques DDoS d'ampleur visant des infrastructures de télécommunications ont eu des conséquences importantes sur la disponibilité de services critiques.

L'ANSSI remarque également que le « ciblage d'opérateurs de télécommunications à des fins d'espionnage est intense ». Ces deux dernières années, l'ANSSI a ainsi traité plusieurs incidents affectant des entités du secteur des télécommunications en France à des fins d'espionnage.

Nous avons le plaisir d'accueillir pour la fédération française des télécoms (FFT) : M. Patrick Guyonneau, président de la commission sécurité de la FFT et directeur de la sécurité du groupe Orange, M. Matthieu Hennebo, directeur cybersécurité d'Altice France – responsable sécurité des systèmes d'information (RSSI) du groupe Altice France et M. Corentin Durand, responsable des affaires publiques de Bouygues Telecom. Le groupe Iliad est représenté par M. Patrice Millecamps, directeur des obligations légales et Mme Ombeline Bartin, directrice des relations extérieures.

Madame, Messieurs, nous serons attentifs à vos retours sur les aspects du projet de loi qui vont concernent particulièrement, en particulier sur les points susceptibles de susciter des interrogations. Nous serons également à l'écoute de vos propositions concrètes pour renforcer la sécurité et la résilience du secteur des télécommunications.

M. Patrick Guyonneau, président de la commission sécurité de la FFT, directeur de la sécurité d'Orange France. Je vous remercie de nous donner l'occasion de nous exprimer sur un texte que nous avons déjà évoqué avec certains d'entre vous. Les opérateurs de télécom ont été diligents vis-à-vis des cybermenaces depuis longtemps, dans la mesure où les cyberattaques quotidiennes ont permis très tôt aux opérateurs d'apprendre à les détecter et à s'organiser pour les contrer. Nous n'avons pas attendu le projet de loi pour adopter des pratiques, des mesures très strictes et pertinentes en matière de cybersécurité en fonction des analyses de risque, notamment pour nos systèmes d'information les plus sensibles, dont les dysfonctionnements engendrent un impact transverse très important sur la continuité d'activité des opérateurs.

Ces mesures ont été renforcées par les contraintes ajoutées par le code de la défense après la loi de programmation militaire (LPM) de 2013. La plupart des opérateurs sont ainsi

devenus des acteurs très régulés, différentes réglementations européennes et nationales s'imposant à nous. Ces liens étroits avec nos autorités de tutelle, en particulier l'Anssi, en témoignent et permettent aux opérateurs de délivrer à votre commission un certain nombre de messages tirés de nos expériences. Nous avons fortement conscience des menaces systémiques qui pèsent sur nous, comme sur de nombreux autres industriels ou opérateurs de services, mais aussi des menaces très ciblées.

L'actualité démontre malheureusement que les opérateurs sont fortement ciblés. Par ailleurs, nous savons que le risque zéro n'existe pas. En conséquence, nous souhaitons participer à cet effort commun de rehaussement du niveau de cybersécurité. J'ajoute deux arguments importants sur le soutien à cette démarche d'ensemble. D'abord, nous faisons appel à un grand nombre de sous-traitants ou de prestataires dont le niveau de cybersécurité est très hétérogène. Nous avons donc intérêt à ce qu'il s'améliore. Ensuite, en raison de leur longue expérience, tous les opérateurs de télécommunication ont en général développé une forme d'activité *BtoB* dans ces domaines.

En revanche, lors de notre audition devant la commission supérieure du numérique et des postes (CSNP), représentée ici par Mme la députée Le Hénanff, mais aussi au Sénat, nous nous étions inquiétés d'une surtransposition législative, au sens d'une transposition maximaliste par le haut. Dans la première version du texte, les difficultés d'interprétation pouvaient être sources d'insécurité juridique. Cette surtransposition aurait conduit à porter atteinte à la compétitivité des entreprises françaises et, *in fine*, à l'objectif d'harmonisation européenne. Nous remercions la CSNP et le Sénat d'avoir accepté un certain nombre d'amendements qui vont dans le bon sens selon nous.

Aujourd'hui, nous voudrions vous alerter sur l'une des principales questions posées aujourd'hui par ce projet de loi. Elle n'est d'ailleurs pas directement dans la loi, mais d'ordre réglementaire. Il s'agit du référentiel de mesures de cybersécurité, qui sera publié par l'Anssi. Ce référentiel, et notamment les règles prévues par l'article 14, n'est pas forcément utile pour tous les systèmes d'information de nos entreprises. Si notre cœur d'activité mérite sans doute de disposer d'un référentiel de haut niveau, toute la complexité ne peut pas être portée par l'ensemble des systèmes d'information.

Le texte de l'Anssi n'exige une conformité que pour les objectifs à respecter, mais en cas de contentieux avec nos clients, la difficulté réside pour nous dans cet objectif de résultat, potentiellement source d'une grande incertitude quant à sa portée et sa valeur. De plus, le principe de proportionnalité mis en avant par le directeur général de l'Anssi lors de son audition devant votre commission n'est pas encore suffisamment inscrit dans la loi à notre sens, malgré l'amendement sénatorial sur l'article 14.

Le changement d'échelle, avec l'assujettissement de NIS 2 à tous les systèmes d'information (SI), quelle que soit leur criticité, est problématique et nous semble contraire au principe de proportionnalité : toutes les activités des opérateurs ne peuvent être placées au même niveau de résilience.

Normalement, des analyses doivent être conduites par l'État et être transcrites dans une directive nationale de sécurité pour chaque secteur d'activité, pour nous permettre d'orienter nos efforts et nous focaliser là où ils sont le plus nécessaires. Le principe de mise en œuvre pour tous les niveaux d'exigence technique ne doit pas seulement s'appliquer sur les types d'entités. Ce n'est pas tant la taille de l'entité qui importe, mais la sensibilité des SI et l'impact en cas de dysfonctionnement.

Ensuite, la plupart d'entre nous sommes présents dans plusieurs pays européens. Nous avons ainsi pu constater comment d'autres pays ont transposé la directive NIS 2, laissant le soin aux acteurs d'apprécier leurs besoins par des analyses de risque et d'adopter des mesures strictement nécessaires en co-construction avec les autorités de tutelle. Il est hors de notre portée de réaliser pour l'ensemble de nos systèmes d'information des audits obligatoires, de déployer les mesures les plus complexes, comme des réseaux spécifiques d'administration, des postes spécifiques pour les administrateurs. Ce sont ces questions de mise en conformité qui nous posent problème, surtout dans des délais extrêmement réduits, puisqu'ils sont de l'ordre de trois ans. L'application des mesures les plus strictes occasionnerait environ 20 % de surcoûts pour un SI, à la fois dans la conception, mais aussi dans le maintien en condition quotidienne. Or nous avons déjà consenti des investissements massifs pour d'autres raisons et notre secteur connaît actuellement une situation économique difficile.

Ensuite, nous nous interrogeons sur le niveau de sévérité des incidents à déclarer, dans la mesure où tout incident cyber est susceptible d'engendrer de grandes conséquences. Il est donc difficile pour nous de cerner exactement ce que nous devrons signaler à l'Anssi, dans des délais très contraints, qui ne nous permettront pas de conduire des analyses d'impact suffisantes.

Nos principales recommandations reposent sur une priorisation et une hiérarchisation dans un souci de proportionnalité des exigences, afin d'éviter la congestion et des surcoûts. Nous souhaitons également échelonner dans le temps la mise en œuvre de ces mesures techniques ou organisationnelles. Ensuite, des mises en œuvre d'accords de reconnaissance mutuelle permettraient aux organisations de satisfaire aux exigences de l'Anssi dans plusieurs États membres qui se contentent d'une conformité à ISO 27000.

S'agissant des incidents importants, nous souhaiterions que des critères plus précis soient établis avant d'enclencher une notification, sous peine d'engorger le système de l'Anssi. Nous estimons également qu'un organe de supervision parlementaire sur la mise en œuvre de ces règles NIS 2 pourrait représenter une bonne solution, afin d'éviter une surtransposition uniquement administrative.

Malgré la qualification par l'Anssi de notre secteur comme « supercritique », les pouvoirs publics n'ont pas pour l'instant classé les télécoms au rang de services essentiels dans notre pays, notamment dans l'arrêté du 5 juillet 1990, fixant les consignes générales de délestage des réseaux électriques. Le rapporteur Éric Bothorel rappelait à juste titre lors de l'audition du secrétariat général pour la défense et la sécurité nationale (SGDSN) l'importance des systèmes de télécommunication pour la résilience de l'ensemble des entités.

M. Matthieu Hennebo, directeur cybersécurité d'Altice France. La notion de proportionnalité concerne les mesures de sécurité que nous pourrions être conduits à identifier et à devoir mettre en œuvre sur ces systèmes en fonction de la criticité des services qu'ils délivrent. La proportionnalité porte également sur leur délimitation dans le cadre de la mise en œuvre des mesures de cybersécurité.

M. Corentin Durand, responsable des affaires publiques de Bouygues Telecom. Je partage les propos du président de la commission sécurité de la FFT et me permets d'insister une nouvelle fois sur les notions de priorisation et de proportionnalité.

Aujourd'hui, un opérateur comme Bouygues Télécom opère sur des milliers de systèmes d'information, des services qui sont essentiels, aussi bien pour les citoyens que pour les entreprises avec lesquelles nous travaillons. Ces systèmes d'information doivent être robustes et évidemment protégés. Cependant, les systèmes d'information sur lesquels nous opérons aujourd'hui ne peuvent pas tous être considérés comme critiques.

Dans notre entreprise, nous avons défini une forme de nomenclature de sensibilité des applications et systèmes d'information avec lesquelles nous travaillons quotidiennement pour les activités que nous gérons, c'est-à-dire des activités réseaux généralement critiques, ou des activités indépendantes des activités réseaux, sur lesquelles la compromission n'aura pas du tout le même impact.

Il existe quatre typologies de sensibilité. Un certain nombre de systèmes d'information sont non-sensibles, puisque leur compromission ne provoquerait pas de problèmes graves ou alors modérés et qui ne remettraient pas nécessairement en question notre activité ou des activités qui existent grâce à nous.

En revanche, sur deux niveaux de sensibilité élevés, voire très sensibles, les règles les plus strictes doivent s'appliquer, y compris les analyses de risque qui nous paraissent absolument essentielles sur ces types de systèmes d'information, mais qui ne provoqueraient pas de problèmes graves, disproportionnés, en cas de compromission. C'est la raison pour laquelle nous parlons effectivement de proportionnalité jusqu'à présent, en sachant que la proportion de systèmes d'information que nous pourrions considérer comme sensibles et très sensibles est plutôt limitée et que de nombreuses applications aux SI ne rentrent pas dans ces deux catégories.

Patrick Guyonneau a évoqué le sujet de la qualification des opérateurs télécoms comme des services prioritaires. Lors de l'hiver 2022-2023, voire de l'hiver 2023-2024 dans une moindre mesure, nous avons ainsi été quelque peu surpris d'apprendre que nos infrastructures pourraient potentiellement faire l'objet de délestages électriques, non seulement parce que nous sommes aussi dans l'obligation d'assurer en permanence l'acheminement de nos communications d'urgence – une activité absolument essentielle – mais aussi parce que les infrastructures télécoms sont absolument incontournables.

Le deuxième élément de cette priorisation concerne la réaction qui devrait être la nôtre à l'occasion d'incidents climatiques. Nous en avons connu un certain nombre récemment et nous serons probablement conduits à en connaître de plus en plus. Dans ces circonstances, certaines de nos antennes finissent par ne plus fonctionner, parce qu'elles subissent une rupture d'alimentation électrique. Il s'agit non seulement de sécuriser nos antennes et le réseau électrique, mais surtout de nous assurer que ces infrastructures soient de nouveau alimentées dès le déploiement de la réponse de crise. Nous estimons qu'il faut effectivement relever le niveau de sécurisation des infrastructures supercritiques.

Mme Ombeline Bartin, directrice des relations extérieures d'Iliad-Free. Je partage l'ensemble des préoccupations qui ont pu être soulignées par la FFT et les différents opérateurs. En synthèse, ce texte comporte trois enjeux principaux pour nous.

En premier lieu, il faut nous laisser le temps de la mise en œuvre du texte. Le directeur général de l'Anssi avait évoqué trois ans, ce qui constitue une durée minimale. En effet, si les opérateurs entreprennent depuis plusieurs années des mesures d'audit, de prévention et de sécurisation de leurs SI, le texte de transposition nous fait changer d'échelle.

En conséquence, il serait plus sécurisant pour nous que la loi inscrive un délai de mise en œuvre, comme cela peut être le cas pour d'autres dispositions du texte.

Deuxièmement, toute surtransposition engendrerait pour nous des complexités et des coûts supplémentaires. Or, la mise en conformité avec ce nouveau texte de l'ensemble de nos SI sera déjà assez coûteuse.

Troisièmement, le projet de loi prévoit de nombreux renvois à des décrets sur des points substantiels, notamment le référentiel ou des procédures de notification. Ces recours constituent pour nous une source d'insécurité ; nous préférerions savoir dès le départ les règles que nous devrons appliquer, les procédures que nous devrons respecter. Nous préconisons donc de simplifier le plus possible le recours à ces décrets.

Un autre point d'attention est lié au référentiel évoqué à l'article 14. La définition de ce référentiel représentera un enjeu considérable pour nous, d'autant plus qu'aujourd'hui, la norme ISO 27001 prévoit des procédures que nous respectons d'ores et déjà. Enfin, le dernier élément concerne l'article 17. Il serait sécurisant de déterminer un point unique de notification des incidents et des vulnérabilités. À l'heure actuelle, il existe en effet une multiplicité de procédures entre Bercy, le ministère de l'intérieur et l'Anssi.

En conclusion, je souligne que la rédaction par le Sénat porte également des avancées, notamment la reprise des définitions des incidents et des vulnérabilités et la précision des délais de la procédure graduée prévue par la directive. Nous demandons à l'Assemblée nationale de conserver ces points qui offrent une meilleure visibilité et une meilleure définition de l'objet des procédures impliquées.

M. Éric Bothorel, rapporteur général. Madame Bartin, vous venez d'évoquer votre attachement à un délai de mise en œuvre. Je me permets de souligner que vous avez déjà gagné un an, puisque nous examinons un texte qui aurait dû être adopté l'année dernière. Même si la version définitive du texte n'est pas stabilisée, ses grandes lignes sont connues de longue date, me semble-t-il.

Parmi les priorités 2022-2027 des opérateurs télécoms présentées par la FTT, la proposition n° 2 vise à « *intensifier la prévention et la lutte contre les actes de malveillance et de dégradation des infrastructures numériques en renforçant les réquisitions en diversifiant les sanctions pénales à l'encontre de leurs auteurs* ». La proposition n° 6 consiste à « *évaluer la conformité, d'une part des actes législatifs existants, et d'autre part de toute réforme, au principe de concurrence équitable (*level playing field*) avec les autres acteurs du numérique afin de ne plus créer de nouveaux écarts entre les acteurs, généraliser les études d'impact ex ante et ex post sur ces sujets* ». La proposition n° 7 a pour objet de *« poursuivre les travaux de réforme de la directive NIS afin que les éditeurs de logiciels d'importance stratégique et les équipementiers soient responsabilisés au même titre que les opérateurs télécoms* ».

La multiplication du nombre d'acteurs concernés par les directives NIS 2 et REC est patente, y compris le secteur public. Vous avez développé selon vos propres termes une sécurité robuste en faveur de la résilience de l'intégralité de la chaîne de valeur. Or nous entendons qu'il faudrait être plus souple avec les filiales, tout en étant plus exigeant avec les sous-traitants. Quel est votre point de vue à ce sujet ?

Ensuite, vous êtes des entreprises de télécoms, mais une partie des réseaux sont sous statut public. Le Sénat semble attentif à ce que le projet de loi n'ait pas un impact trop fort les

collectivités. Qu'en pensez-vous ? Enfin, les asymétries réglementaires entre opérateurs télécoms et géants d'internet perdurent. Vous nous avez régulièrement interpellés afin qu'elles soient impérativement corrigées pour assurer un traitement équitable de tous les acteurs de l'écosystème numérique. Pensez-vous que les dispositions de ce projet de loi puissent y contribuer ?

Mme Anne Le Hénanff, rapporteure. Les modifications apportées par le Sénat à ce stade vous conviennent-elles ? Faut-il préciser encore plus quelques notions ?

Ensuite, les procédures en matière de gestion de crise sont-elles spécifiques à chacune de vos entreprises ou existe-t-il un référentiel commun, par exemple sous l'égide de la FFT ? Comment vous inscrivez-vous dans des procédures telles que les plans communaux, départementaux ou préfectoraux de sauvegarde ? Le texte doit-il approfondir la gestion de crise et des moyens à mettre en œuvre pour vous guider ? Ce texte vous conduira-t-il à faire évoluer vos procédures collectives ou individuelles ?

Enfin, M. Guyonneau, vous avez souligné l'importance à vos yeux de l'idée de proportionnalité, en fonction de la taille des opérateurs. Pourriez-vous nous fournir des exemples précis ? Quels risques distinguent un petit opérateur télécom d'un opérateur de plus grande taille ?

M. Patrick Guyonneau. Chaque opérateur dispose de ses propres procédures de gestion de crise, pour différentes raisons. Cependant, nous avons fortement travaillé sur nos procédures avec l'État, en particulier le commissariat aux communications électroniques de défense (CCED) et le centre opérationnel de gestion interministérielle des crises (Cogic). Nous avons ainsi produit des efforts, qui ont été salués, sur la rapidité de prévention et l'impact estimé de tel ou tel incident. En conséquence, il ne semble pas nécessaire que la loi apporte des compléments à ce sujet.

Par ailleurs, nous échangeons en temps réel entre opérateurs, dès que l'un d'entre nous souffre d'un incident. Les Jeux olympiques, qui se sont déroulés avec succès, ont d'ailleurs prouvé la validité de nos procédures face aux incidents qui se sont produits. En revanche, comme le soulignait Mme Ombeline Bartin, nous sommes demandeurs d'un interlocuteur unique dans le cadre du signalement des incidents.

Je ne pense pas que la taille des opérateurs soit l'élément le plus discriminant. Cela dépend de leur place dans le service que l'État juge essentiel ou critique pour la résilience de la société. Un petit opérateur peut être fondamental dans le transport de la donnée, par exemple sur une zone très particulière. À ce sujet, et pour répondre à une question du rapporteur Bothorel, tout n'est pas réglé vis-à-vis des sous-traitants ou des concurrents. Pour l'instant, un certain nombre de partenaires industriels, ne sont pas forcément visés dans cette chaîne, lorsque l'on réfléchit à la résilience de bout en bout.

Enfin, je précise que nous conduisons des exercices réguliers avec les différents organismes de l'État.

M. le président Philippe Latombe. S'agissant de la directive sur la résilience opérationnelle numérique du secteur financier (Dora), avez-vous d'autres points à apporter à notre connaissance concernant le titre III ?

M. Matthieu Hennebo. Les opérateurs télécom délivrent des prestations et des services à de nombreuses entreprises du secteur bancaire et assurantiel. À ce titre, une source d'inquiétude concerne la capacité qui sera laissée à ces clients de pouvoir opérer des audits assez larges, dans le cadre de Dora.

Nous souhaiterions obtenir plus de lisibilité sur l'encadrement applicable à ces échanges qui, rappelons-le, restent d'ordre commercial. Il s'agirait d'obtenir des précisions sur les systèmes à auditer, leur périmètre ; mais également le niveau d'accès aux informations accordé. En effet, si le service est effectivement « sensible », faudra-t-il donner l'accès à des informations très sensibles ? Il s'agit là d'un point de vigilance sur l'application et la transposition de Dora, mais aussi les contractualisations qui en découleront.

M. Corentin Durand. Dora placera au centre du jeu de nouvelles autorités de régulation du secteur financier, en toute logique. Je partage à ce titre les propos du directeur de l'Anssi, quand il indique que son agence ne doit pas être exclue de l'application de ce règlement. En effet, nous serons concernés par les audits potentiels et avons besoin que l'autorité de tutelle avec laquelle nous avons l'habitude de travailler soit concernée, au titre de la réponse aux incidents ou tout simplement pour le suivi de l'interfaçage entre les réglementations NIS 2 et Dora.

M. le rapporteur général Bothorel, nous n'avons pas à ce jour d'avis sur les obligations des collectivités. Cependant, étant confrontés à la même problématique, nous constatons que la marche demeure assez haute. J'en profite également pour souligner les actions des opérateurs en matière de développement d'offres de diagnostic et de programmes de mise en conformité qui s'adressent non seulement aux nouvelles entités qui seront assujetties à NIS 2, mais aussi aux collectivités. Si ces dernières ressentent le besoin d'être accompagnées, nous nous tiendrons à leur disposition.

M. le président Philippe Latombe. Si je comprends bien, deux questions se posent pour vous dans le cadre de Dora. La première concerne les audits et votre assujettissement à l'Autorité des marchés financiers (AMF) et à l'Autorité de contrôle prudentiel et de résolution (ACPR), ce qui n'était pas le cas auparavant, puisque l'Anssi était votre seul interlocuteur.

La deuxième est liée à la faculté des sociétés soumises à Dora d'auditer les entreprises avec lesquelles elles travaillent, dans un cadre contractuel. Vous redoutez que ces sociétés vous imposent des audits réguliers, potentiellement sur des systèmes d'information qui ne les concernent pas, mais qu'il pourrait être important pour vous de conserver à titre confidentiel ou, à tout le moins, de ne pas trop les exposer. Ai-je bien résumé la situation ?

M. Matthieu Hennebo. Exactement. Il s'agit de bien recentrer cette notion d'audit et la sensibilité de certains systèmes et services qui pouvaient être délivrés. Aujourd'hui, la criticité ne porte pas sur le service à proprement parler, mais sur l'opérateur. Il faudrait donc opérer un cadrage, notamment au niveau du service qui est concrètement mis à disposition du client bancaire. Simultanément, l'Anssi devrait être en mesure d'arbitrer la notion d'audit ou la capacité à pouvoir donner accès à certaines informations de systèmes sensibles.

Notre interrogation porte donc sur les critères selon lesquels un opérateur sera jugé critique par une banque. S'agira-t-il de son service ? La catégorisation sera-t-elle établie par une autorité européenne ou nationale de surveillance, en l'occurrence l'AMF ou l'ACPR ?

M. le président Philippe Latombe. Identifiez-vous dans le texte des éléments sur lesquels il faudrait apporter des précisions et, si tel est le cas, lesquelles seraient-elles ? En effet, selon que la loi se concentre sur la notion de service ou d'opérateur, les champs sont totalement différents. Nous devons absolument éviter les effets de bord, d'autant plus qu'il s'agit d'une transposition et non uniquement d'une loi d'initiative française.

M. Corentin Durand. À ce stade, il s'agit surtout pour nous d'une alerte, que nous n'avions pas initialement identifiée sur ce texte. Je ne suis pas certain que la réponse à la question de la criticité des services de connectivité doive être d'ordre législatif, compte tenu de la technicité des sujets. En revanche, ce sujet ne doit pas être oublié et nous espérons pouvoir le retravailler. Au-delà, il nous semble essentiel que notre autorité de tutelle habituelle, l'Anssi, puisse être réellement impliquée dans la mise en œuvre de Dora. Cela nous faciliterait la tâche.

M. Éric Bothorel, rapporteur général. Madame Bartin, qu'entendez-vous par « simplifier le recours aux décrets » ? Faut-il inscrire dans le droit le référentiel ou la procédure de notification ? J'aimerais obtenir des éclaircissements sur cet aspect.

M. le président Philippe Latombe. Je prolonge la question du rapporteur général. Les précisions que vous avez évoquées concernant Dora devraient-elles être inscrites dans la loi ? *A priori*, cela relèverait plutôt du domaine du réglementaire, mais dans vos propos liminaires, vous indiquiez votre souhait de voir la partie réglementaire limitée.

Ces aspects n'avaient pas été mentionnés lors des auditions du Sénat. Or nous intervenons dans le cadre d'une procédure accélérée et nous allons devoir nous accorder avec les sénateurs. Cela implique de parvenir à une écriture la plus précise possible, afin de faciliter le travail de la commission mixte paritaire (CMP). Mes demandes de précision ont pour objet de permettre aux sénateurs d'y réfléchir de leur côté, avant la CMP.

Mme Ombeline Bartin. Certaines mesures ne peuvent effectivement être définies que par voie réglementaire. Simplement, nous souhaitons pouvoir les anticiper au maximum, ce qui n'est pas le cas aujourd'hui. S'agissant du référentiel, nous souhaitons nous assurer qu'il correspondra bien à la norme ISO 27 001.

Les procédures de notification sont assez bien définies dans le texte de loi et dans la directive. En conséquence, nous nous demandons quelles précisions pourraient être apportées par voie réglementaire, dans la mesure où les procédures en vigueur aujourd'hui fonctionnent et ont fait leur preuve.

M. le président Philippe Latombe. Si je comprends bien, vous seriez favorable à une démarche similaire à celle employée par les Belges, c'est-à-dire transposer en faisant immédiatement référence à ISO 27001, plutôt que d'établir un autre référentiel.

Mme Ombeline Bartin. Oui.

M. Patrick Guyonneau. D'une certaine manière, oui. À tout le moins, nous souhaiterions qu'il existe des équivalences, telles que celles mentionnées par l'Anssi. Ainsi, le respect de l'ISO 27001 offrirait une présomption de conformité. Cette question rejoint celle de la proportionnalité dans les services rendus. En effet, les systèmes d'information se comptent par milliers et n'ont pas tous le même degré d'importance ni de sensibilité. C'est la

raison pour laquelle, avant de parvenir au référentiel de l'Anssi, il est nécessaire de disposer d'un décret qui précise cette proportionnalité par rapport à la criticité du service rendu.

Il s'agit d'éviter des situations rocambolesques pour tous les opérateurs paneuropéens. Par exemple, notre filiale belge *BtoB* pourrait travailler en France grâce à une présomption forte de compatibilité NIS parce qu'elle est ISO 27001 en Belgique, quand cela ne serait pas le cas d'Orange Business France, qui n'aurait pas encore intégralement coché toutes les cases du référentiel Anssi. Le problème porte bien sur la gestion de la cohérence.

Ensuite, les articles 14 et 17 posent question, en particulier sur les pertes financières. Nous ne sommes pas en mesure d'évaluer la matérialité des impacts financiers pour un certain nombre de clients. Plus précisément, il s'agit de l'alinéa 3 de l'article 17. Selon nous, il mériterait sans doute d'être rédigé différemment et plutôt parler de l'impact sur le service. La résilience n'équivaut pas à un risque zéro, mais concerne la continuité de service. À titre d'illustration, en cas de crise, l'accès à internet n'a pas la même importance selon qu'il s'agit d'un particulier ou d'un hôpital.

Une question du même ordre se pose à l'article 14, concernant les conséquences économiques et sociales. En gestion de crise, lorsqu'un incident survient, et compte tenu des délais imposés pour effectuer les déclarations, nous sommes incapables de nous occuper des conséquences économiques et sociales. Dans de telles circonstances, notre principale préoccupation consiste à rétablir le service, avec une priorité accordée aux numéros d'urgence.

En résumé, il conviendrait de clarifier ce qui est considéré comme « essentiel » dans les articles 14 et 17 ou, à tout le moins, renvoyer à un premier décret. En effet, je ne partage pas l'idée selon laquelle nous aurions le temps pour la mise en application. De fait, les délais courent depuis le 17 octobre de l'année de la publication de la directive. Pour certains sujets, le chronomètre est déjà enclenché, mais nous ne savons pas ce que nous devons faire.

M. Éric Bothorel, rapporteur général. Quel est votre point de vue concernant la sanction pénale des dirigeants ?

M. Patrick Guyonneau. Ici aussi, il existe un enjeu d'harmonisation et de cohérence, puisque le texte ne prévoit pas de sanction pénale pour un haut fonctionnaire qui n'aurait pas agi comme il le devait en matière de systèmes d'information. En effet, certaines données des ministères sont plus sensibles que celles que nous détenons. Soyez rassurés, chez tous les opérateurs, les sujets de sécurité sont extrêmement importants. Nos comités exécutifs les abordent et les font figurer au rang des priorités lors des analyses de risques.

M. Corentin Durand. Le secteur des télécoms est extrêmement régulé et il existe déjà de nombreux textes qui prévoient d'engager la responsabilité des dirigeants en cas de non-respect des obligations qui leur incombent. Je partage le point de vue de M. Guyonneau : les enjeux cyber figurent parmi les priorités, au quotidien.

M. le président Philippe Latombe. Nous avons évoqué la problématique de Dora et la question de l'assujettissement indirect. Existe-t-il des zones de frottement, des incompatibilités, entre NIS 2 et la directive REC vous concernant ? Entre le texte de loi et d'autres réglementations comme le règlement général sur la protection des données (RGPD), par exemple ?

M. Patrick Guyonneau. Non, pas à ma connaissance, hormis le sujet du *non bis in idem* ; nous ne voulons pas être punis deux fois. Ensuite, un incident peut engendrer de multiples conséquences. En fonction du type de conséquence, plusieurs personnes doivent être alertées et nous sommes préoccupés à l'idée d'en oublier une.

S'agissant de Dora, la plupart des clients bancaires ne réalisent pas eux-mêmes les audits, mais font appel à des cabinets ou des prestataires extérieurs. À ce titre, nous ne souhaitons pas devoir multiplier les audits, *a fortiori* avec des acteurs qui ne seraient pas forcément nationaux ou européens.

M. le président Philippe Latombe. Considérez-vous que le sujet du *non bis in idem* est aujourd'hui traité dans le texte issu du Sénat ?

M. Patrick Guyonneau. Il me semble que cet aspect a été clairement traité par M. Strubel, qui a indiqué qu'il n'y aurait pas de double sanction. Nous estimons que vous envisagerez cet aspect avec sagesse, dans le texte.

M. Éric Bothorel, rapporteur général. Avez-vous identifié des points de frottement entre le projet de loi tel qu'il a été rédigé par le Sénat et d'éventuelles dispositions du règlement européen sur la cyberrésilience (Cyber Resilience Act, CRA) ?

M. Patrick Guyonneau. Il est encore un peu trop tôt pour nous prononcer à ce sujet, nous sommes en train d'étudier le CRA, qui porte des sujets importants vis-à-vis d'un certain nombre de nos équipements.

M. le président Philippe Latombe. Si vous identifiez rapidement des éléments, nous vous serions reconnaissants de nous en faire part, afin que nous puissions anticiper au maximum d'éventuels frottements, à plus forte raison si le texte est examiné en septembre dans l'hémicycle.

M. Matthieu Hennebo. S'agissant de Dora, je souscris aux propos de M. Guyonneau concernant l'accès d'auditeurs étrangers à des informations sensibles. Un opérateur pourra être soumis à Dora dans la mesure où il délivre des services à une banque ou une assurance. Sans entrer dans des considérations très techniques et complexes qu'il n'est pas envisageable d'intégrer dans la loi, nous souhaiterions bénéficier de suffisamment de visibilité, de cohérence. Par exemple, il serait utile que l'Anssi puisse à un moment donné se prononcer pour confirmer qu'un service délivré par l'opérateur pour la banque dans tel ou tel contexte est critique ou non.

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

La séance est levée à 18 heures 05.

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 mercredi 4 juin 2025 à 17 heures

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