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

Mardi 8 juillet 2025
Séance de 18 heures

Compte rendu n° 12

SESSION EXTRAORDINAIRE DE 2024 - 2025

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-huit heures dix

La commission spéciale a auditionné Mme Laure de La Raudière, présidente de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) et M. Olivier Corolleur, directeur général de l'Autorité.

M. le président Philippe Latombe. Je souhaiterais tout d'abord évoquer le calendrier d'examen du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. La commission spéciale l'examinera à partir du mardi 9 septembre. L'examen en séance publique est, à ce stade, prévu au début de la session extraordinaire qui devrait s'ouvrir le lundi 22 septembre.

Nous poursuivons nos auditions en recevant la présidente et le directeur général de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep).

Le Panorama de la cybermenace 2024 de l'Agence nationale de la sécurité des systèmes d'information (Anssi) illustre la diversité et la gravité des menaces qui pèsent, entre autres, sur le secteur des télécommunications. Cette étude distingue les menaces à visée lucrative, celles qui ont une finalité d'espionnage et celles qui visent à déstabiliser nos sociétés, les actes de sabotage relevant de cette dernière catégorie. 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 par déni de service distribué (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'Agence a ainsi traité plusieurs incidents affectant des entités du secteur des télécommunications en France à des fins d'espionnage.

Le projet de loi que la commission spéciale est chargée d'examiner comporte trois titres. Le titre I^{er}, consacré à la résilience des activités d'importance vitale, procède à la transposition de la directive sur la résilience des entités critiques (REC). Mme Catherine Hervieu en est la rapporteure. Le titre II vise à renforcer notre cadre juridique en matière de cybersécurité et procède à la transposition de la directive NIS 2, relative à la sécurité des réseaux et des systèmes d'information. Sa rapporteure thématique est Mme Anne Le Hénanff. Enfin, le titre III est consacré à la résilience opérationnelle numérique du secteur financier et procède à la transposition du règlement sur la résilience opérationnelle numérique du secteur financier, dit Dora. M. Mickaël Bouloux en est le rapporteur. M. Éric Bothorel, quant à lui, est le rapporteur général du projet de loi.

Mme Laure de La Raudière, présidente de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. Je suis accompagnée d'Olivier Corolleur, directeur général de l'Autorité, et de Virginie Mathot, ma conseillère à la présidence.

Dans le cadre de notre saisine pour avis sur le projet de loi, nous nous sommes concentrés sur les mesures qui s'appliquent spécifiquement au secteur que nous régulons, à savoir celles qui ont trait à la transposition de la directive NIS 2, à l'accès aux fréquences par les terminaux satellitaires terrestres et aux sanctions contre les auteurs de brouillages qui créent un préjudice. Nous nous sommes penchés notamment sur les questions qui pourraient

avoir un impact, d'une part, sur le bon fonctionnement des réseaux et des services de communications électroniques, d'autre part, sur la sécurité juridique dont doivent bénéficier les opérateurs dans la mise en œuvre de leur obligation légale.

En comparaison de NIS, la directive NIS 2 s'applique à un éventail beaucoup plus large d'opérateurs : l'ensemble d'entre eux, quelle que soit leur taille, sont concernés – je ne parle pas des opérateurs d'importance vitale (OIV), qui sont couverts par le secret-défense et dont l'Arcep n'a pas à connaître. Dans le cadre de NIS, seuls les fournisseurs de DNS (systèmes de noms de domaine) et les points d'échange internet (IXP) étaient susceptibles de relever du périmètre des acteurs régulés au titre des opérateurs de services essentiels.

Dans le cadre de NIS 2, on parle d'entités essentielles et d'entités importantes – la catégorisation dépendant notamment de leur taille – mais tout le secteur des communications électroniques est concerné. Parmi les secteurs que nous régulons figurent les fournisseurs de services d'informatique en nuage, qui font partie du secteur hautement critique des infrastructures numériques et qui seront assujettis aux obligations de NIS 2, au même titre que les entités des services postaux et du courrier.

Les entités concernées se caractérisent donc par leur très grande diversité : dans le secteur que nous régulons, la directive s'applique à de très grands groupes comme à des entreprises de toute petite taille. À cet égard, nous appelons votre attention sur l'exigence de proportionnalité énoncée par la directive et rappelée par le Sénat à l'article 14 du projet de loi. Nous estimons qu'elle devrait être appréciée finement, en cohérence avec les moyens réels des entités assujetties.

Nous souhaitons également insister sur le délai de mise en conformité. Celle-ci nécessite en effet un effort substantiel en raison de l'ampleur des adaptations requises pour de nombreux acteurs. C'est valable pour les entités nouvellement assujetties – je pense aux très petites, petites et moyennes entreprises (TPE-PME), qui sont généralement les moins matures en matière de cybersécurité – mais cela peut aussi concerner les OIV ou les anciens opérateurs de services essentiels. Le champ d'application de NIS 2 étant beaucoup plus étendu que celui de NIS, c'est l'ensemble des systèmes d'information de l'entreprise qui sont concernés et non pas les seuls systèmes informatiques des infrastructures numériques sensibles.

C'est pourquoi, dans notre avis, nous avions appelé le gouvernement à prévoir une entrée en vigueur différée du projet de loi afin de laisser le temps aux acteurs de se conformer aux exigences de la nouvelle réglementation. Le gouvernement et le Parlement n'ont pas, pour l'instant, donné suite à cette demande. Toutefois, nos échanges avec l'Anssi ont mis en lumière le fait que l'Agence tiendrait compte de la capacité réelle des entités soumises à NIS 2 à respecter les obligations définies par le texte.

Nous avons aussi relevé des difficultés dans les critères d'assujettissement prévus par le projet de loi, notamment pour les entités implantées dans plusieurs pays ou qui y exercent différentes activités. Sur ce point, le projet de loi se borne à reprendre les critères de la directive sans apporter de précision, ce qui laisse perdurer des incertitudes. L'Anssi a indiqué que les textes réglementaires y répondraient en partie et qu'il était préférable de leur laisser le soin de préciser cette question, ce qui me paraît de bonne pratique.

Nous ne sommes pas directement concernés par NIS 2 puisque c'est l'Anssi qui mettra en œuvre la directive mais je voulais vous alerter sur l'ampleur de ce changement pour le secteur que nous régulons, laquelle variera néanmoins selon la taille des acteurs.

M. Éric Bothorel, rapporteur général. Le manifeste de l'Arcep commence par ces mots : « Les infrastructures numériques que sont les réseaux d'échanges internet, télécoms fixes, mobiles, les centres de données, ainsi que les réseaux postaux et de distribution de la presse, constituent des "infrastructures de libertés". Liberté d'expression et de communication, liberté d'accès au savoir et de partage, liberté d'entreprise et d'innovation qui sont autant d'enjeux clés pour le développement économique et la cohésion de notre pays au sein de l'Europe. » Je tiens à saluer ces termes car j'entends surtout parler, en ce moment, d'interdiction, de contrôle, de sanction et de surveillance – certes légale. Comment l'Arcep contribuera-t-elle, dans le cadre de nos débats, à ce que nous œuvrions à la résilience des infrastructures « de libertés » ?

Vous avez produit, en mai, une note intitulée « La résilience des réseaux de communications électroniques », dans le cadre de votre cycle de réflexion « Réseaux du futur », dans laquelle vous mettez en exergue trois familles de risques : les risques organisationnels, technologiques et naturels.

Parmi les risques organisationnels, vous relevez notamment la fragmentation des acteurs impliqués dans l'exploitation des réseaux de communications électroniques. Du point de vue de l'Arcep, cela a-t-il un impact sur la cybersécurité ? Comment travaillez-vous sur ces questions ?

Compte tenu de l'émergence de nouveaux acteurs impliqués dans l'exploitation d'infrastructures de communications électroniques – je pense en particulier aux TowerCo (Tower Companies) et aux fournisseurs d'offres Telco Cloud –, vous préconisez une revue des obligations pesant sur l'ensemble des acteurs impliqués afin de s'assurer que celles-ci sont appropriées et proportionnées à l'objectif de sécurisation et de résilience. Le cas échéant, vous suggérez d'adapter et de préciser les règles. De votre point de vue, le projet de loi comporterait des lacunes : il ne garantirait pas que tous les opérateurs supportent bien les mêmes obligations. Pourriez-vous apporter des précisions à cet égard ?

S'agissant des risques technologiques, vous soulignez que « la virtualisation et la programmation logicielle des réseaux sont à l'origine d'une mutation profonde des architectures des opérateurs ». C'est un point de vue pertinent, sachant que le projet de loi évoque les infrastructures. Je vous cite encore : « Plus précisément, cette ouverture permet à des tiers (sociétés de services, fournisseurs d'applications, clients industriels /verticaux, MVNO, etc.) d'instancier et d'orchestrer eux-mêmes des services virtualisés. Elle implique donc que de nouveaux acteurs auront accès à certaines données et fonctions liées à l'exploitation du réseau, notamment celles de configuration et de souscription – ce qui relève du suivi de performance, de la supervision et de la maintenance du réseau devrait *a priori* rester sous contrôle exclusif de l'opérateur de réseaux ». À cet égard, des évolutions législatives vous paraissent-elles nécessaires, y compris pour renforcer vos compétences ?

Enfin, concernant les risques naturels, j'ai lu avec intérêt les développements que vous consacriez à l'organisation, aux moyens mis en œuvre et aux retours d'expérience en matière de gestion de crise. Vous citez un passage de la note d'analyse de France Stratégie intitulée « Risques climatiques, réseaux et interdépendances : le temps d'agir » : « les réseaux d'électricité, de transports routier et ferroviaire et de télécommunications […] sont associés, en fonctionnement normal comme en temps de crise, par de nombreux liens de dépendance, physiques ou découlant des relations entre les acteurs. » L'Arcep a-t-elle des recommandations à formuler concernant la gestion de crise et, plus spécifiquement, l'interdépendance des réseaux électriques et de télécommunications ?

Mme Laure de La Raudière. Je voudrais rappeler que l'Arcep est un régulateur économique qui intervient *ex ante* sur les marchés. Autrement dit, nous surveillons les marchés et regardons s'ils présentent des dysfonctionnements sur le plan concurrentiel et si les acteurs se conforment aux principes dont nous devons, de par la loi, contrôler le respect. Nous imposons aux opérateurs, dans un cadre précisément défini, le respect d'obligations d'intérêt général – relatives à l'aménagement du territoire, à la concurrence, à l'innovation, etc. Il s'agit de faire en sorte que les acteurs privés se conforment à ces principes, au-delà de leurs intérêts propres.

Le traitement des enjeux de sécurité et de cybersécurité est de la responsabilité du gouvernement et non de l'Arcep. Comme l'importance que prennent internet et les réseaux sociaux dans la vie sociale et économique ne cesse de croître, nous avons souhaité, en tant qu'experts des télécoms, mettre ce sujet à l'ordre du jour des travaux du comité des réseaux du futur. Le comité réfléchit de manière prospective à certains thèmes qu'il fait exister dans le débat public. L'Arcep n'agit pas dans ce domaine en tant que régulateur économique mais comme expert au service du débat public. L'Autorité a publié en mai une note intitulée « La résilience des réseaux de communications électroniques », puis a organisé, avec la direction générale des entreprises (DGE), un webinaire pour la présenter aux collectivités territoriales. L'objectif est de réfléchir ensemble aux actions à déployer pour conforter la résilience des réseaux. Le comité peut également se pencher sur des sujets relatifs à la cybersécurité, puisque la résilience est aussi celle des réseaux face aux attaques informatiques.

Nous avons soulevé la question de la virtualisation des réseaux : ces derniers intègrent progressivement des logiciels et des fournisseurs différents, lesquels fragilisent les architectures antérieures. Nous alertons ceux qui seront chargés de déployer la directive NIS 2 ainsi que les opérateurs, sur la nécessité de mener un travail fin de détection des nouvelles fragilités des réseaux.

M. le président Philippe Latombe. Des représentants du secteur des télécommunications nous ont fait part, lors d'une audition, de leur souhait d'obtenir des éclaircissements sur le règlement Dora. Les entités soumises à cette norme peuvent diligenter des audits auprès de leurs fournisseurs critiques, dont font partie certains opérateurs de télécommunications.

Ils souhaitent limiter le champ du règlement sur deux points. Tout d'abord, ils veulent que les audits des systèmes d'information ne portent que sur la partie critique de ceux-ci. Ensuite, ils demandent à pouvoir refuser un auditeur pour éviter qu'un cabinet étranger accède à des informations critiques et sensibles. Partagez-vous leurs requêtes ?

Mme Laure de La Raudière. Limiter les audits à la seule partie critique des systèmes d'information me semble logique. Pourquoi les acteurs soumis au règlement Dora auraient-ils besoin d'avoir accès aux services clients ou facturation ? Aux opérateurs de télécommunications de prouver l'étanchéité de leurs systèmes d'information. Il est normal d'auditer la composante qui pilote le cœur du réseau et les équipements de télécommunications qui rendent le service et non celle centrée sur les ressources. L'Anssi est la mieux placée pour répondre à la question, notamment sur le plan technique.

Il pourrait être opportun d'autoriser un tiers à refuser un auditeur pour des raisons tenant à sa nationalité. Cela étant, l'entreprise auditée est forcément juge et partie, donc il faut trouver un dispositif équilibré. Il convient de protéger les audités du risque d'espionnage ou de fuite d'informations vers les concurrents : les auditeurs doivent respecter une déontologie

forte et un acteur extérieur pourrait être chargé de contrôler cette obligation. Le sujet est néanmoins éloigné des compétences de l'Arcep.

M. Olivier Corolleur, directeur général de l'Arcep. Dans la note que vous avez citée, monsieur le rapporteur général, nous pointions principalement la modification de l'organisation du secteur. Ce dernier était animé par quelques opérateurs nationaux ; les responsabilités étaient partagées entre les opérateurs d'infrastructures, les acteurs commerciaux et les fonds d'infrastructures. Notre action consiste à déployer de manière pertinente un dispositif : pour ce faire, il faut bien connaître l'organisation afin de choisir judicieusement les opérateurs d'importance vitale et de définir des obligations générales.

Nous n'identifions pas de lacune dans la directive NIS 2. Pour les raisons que la présidente a exposées dans son propos liminaire, nous ne connaissons pas précisément les choix effectués dans le champ des opérateurs d'importance vitale. Nous devons prendre en compte les bouleversements de l'organisation du secteur dans la désignation des opérateurs les plus sensibles. Le cadre juridique est très complet pour les opérateurs de communications électroniques.

M. Vincent Thiébaut (HOR). Comment évaluez-vous, à l'échelle européenne, le risque lié à notre faible production de matériels d'infrastructures, sachant que les systèmes d'infrastructures utilisés par les opérateurs peuvent presque jouer le rôle de cheval de Troie ?

M. Éric Bothorel, rapporteur général. Les échanges d'informations et de courrier sont couverts par le principe du secret de la correspondance. La loi du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, dite loi « 5G », a rénové ce dispositif. Le Sénat a inséré dans le texte que la commission spéciale est chargée d'examiner une disposition relative à la protection du chiffrement. Jugez-vous cette mesure utile et nécessaire ?

Mme Laure de La Raudière. Monsieur Thiébaut, toute notre économie est exposée au risque de voir des équipements non européens utilisés sur nos réseaux. La question dépasse largement le champ des opérateurs de communication. Je défends la possibilité de privilégier les offres souveraines pour les services les plus critiques. Le rôle de l'Arcep est d'ouvrir les marchés numériques. Ces ouvertures permettent à des acteurs émergents d'apparaître, mais il faut s'assurer que ces derniers offrent des solutions de niveau et de qualité suffisants pour les entreprises. À l'échelle européenne, il convient de donner aux entreprises souveraines accès aux marchés publics. Les marchés privés sont très concurrentiels et les entreprises peuvent avoir peur de tester des solutions par peur de perdre des parts de marché si leur modèle n'est pas le plus avancé ; même si l'exigence de qualité de service est élevée pour les citoyens, les marchés publics sont moins compétitifs, donc ils représentent un domaine intéressant. Dans le secteur des télécoms, deux équipementiers, Ericsson et Nokia, sont européens, donc nous bénéficions d'une certaine protection. Dans une loi qui devait s'appeler la loi Bothorel, on a fait en sorte que tous les équipementiers utilisés par nos opérateurs de télécommunications respectent certaines règles et soient habilités par l'Anssi.

Sur le secret des correspondances, nous sommes très attachés au chiffrement. C'est à la représentation nationale de décider du cadre juridique de celui-ci. L'absence de chiffrement ou l'accès aux clés de chiffrement fragilisent la protection des correspondances.

M. le président Philippe Latombe. Je vous remercie d'avoir répondu à nos questions.

La séance est levée à dix-huit heures trente-cinq.

Membres présents ou excusés

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

Réunion du mardi 8 juillet 2025 à 18 h 00

Présents. - M. Éric Bothorel, M. Tristan Lahais, M. Philippe Latombe, M. Vincent Thiébaut

Excusés. - Mme Marietta Karamanli, Mme Catherine Hervieu, M. Laurent Mazaury