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 3 juin 2025
Séance de 16 heures 30

Compte rendu n° 5

SESSION ORDINAIRE DE **2024 - 2025**

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 16 heures 35

La commission spéciale a organisé une table ronde réunissant les autorités de régulation financière : M. Sébastien Raspiller, secrétaire général de l'Autorité des marchés financiers (AMF), M. Frédéric Hervo, secrétaire général adjoint de l'Autorité de contrôle prudentiel et de résolution (ACPR) et M. Alexandre Garcia, chef de service adjoint du service des affaires internationales de l'ACPR.

M. le président Philippe Latombe. Notre cycle d'auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité s'est jusqu'à présent concentré sur les deux premiers titres du texte. Nous abordons aujourd'hui le titre III, qui transpose dans le droit interne les dispositions de la directive européenne sur la résilience opérationnelle numérique du secteur financier ou Digital Operational Resilience Act, dite Dora. Ce volet relève plus particulièrement de la compétence de notre collègue Mickaël Bouloux, rapporteur thématique ici présent.

Le secteur financier constitue une cible privilégiée pour les cyberattaques. Dans son dernier rapport sur la stabilité financière de décembre 2024, la Banque de France soulignait que le risque de cyberattaques demeurait élevé dans un contexte géopolitique dégradé, se manifestant par diverses menaces hybrides. L'Autorité des marchés financiers (AMF) a d'ailleurs intégré la cybersécurité dans ses contrôles et mené trois campagnes thématiques en 2019, 2020 et 2023.

Nous avons le plaisir d'accueillir l'Autorité des marchés financiers (AMF), représentée par M. Sébastien Raspiller, secrétaire général, et l'Autorité de contrôle prudentiel et de résolution (ACPR), représentée par M. Frédéric Hervo, secrétaire général adjoint et M. Alexandre Garcia, chef de service adjoint du service des affaires internationales.

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi) a exprimé des réserves quant à la simplification opérée par le Sénat concernant l'articulation entre Dora et la directive *Network and Information Security 2* (NIS 2). Il estime que la suppression de la notification des incidents à l'Anssi au profit d'une notification unique aux autorités de contrôle Dora pourrait entraîner des retards préjudiciables, l'Anssi disposant d'un service opérationnel fonctionnant 24 heures sur 24 et 7 jours sur 7, contrairement à l'Autorité de contrôle prudentiel et de résolution (ACPR) et à l'Autorité des marchés financiers (AMF). Partagez-vous cette analyse ? Une double notification via un formulaire unique pourrait-elle constituer une solution plus appropriée ?

M. Frédéric Hervo, secrétaire général adjoint de l'Autorité de contrôle prudentiel et de résolution (ACPR). La résilience cyber et informatique constitue une priorité absolue pour la stabilité financière en France et en Europe, mobilisant quotidiennement nos équipes.

Le secteur financier est en effet confronté à deux défis majeurs dans ce domaine. Tout d'abord, la digitalisation croissante des services financiers, illustrée par l'avènement des paiements instantanés, de la blockchain et de l'intelligence artificielle, a profondément transformé le paysage financier. Cette évolution s'accompagne d'une externalisation accrue des services supports auprès de prestataires spécialisés, notamment dans le domaine du cloud *computing* et des centres de données. La concentration de ces prestataires, souvent des géants technologiques non européens, soulève des enjeux critiques pour le secteur financier. Le cadre

réglementaire Dora est donc essentiel, car il confère aux autorités européennes de supervision, en collaboration avec la Banque centrale européenne et les autorités nationales, des pouvoirs de surveillance sur ces acteurs critiques.

Ensuite, nous observons une recrudescence constante des cyberattaques visant le secteur financier, cible privilégiée des cybercriminels. Un établissement financier insuffisamment protégé peut voir sa solidité financière compromise par une attaque d'envergure. À titre d'exemple, la banque chinoise ICBC a dû recapitaliser sa filiale américaine à hauteur de plusieurs milliards de dollars à la suite d'une attaque par rançongiciel l'année dernière.

Dans ce contexte, le règlement Dora instaure un dispositif reposant sur le triptyque tester, alerter, protéger. Il impose un socle commun d'exigences en matière de gestion des risques informatiques et cyber à l'ensemble des acteurs financiers, des banques aux assureurs, en passant par les infrastructures de marché et les émetteurs de cryptoactifs. Chaque entité doit évaluer sa cyber-résilience, les établissements les plus systémiques étant soumis à des tests d'intrusion renforcés pilotés par leur autorité de contrôle.

Dora prévoit également un cadre harmonisé pour la déclaration et le traitement des incidents cyber. Bien que le règlement soit déjà en application depuis le 17 janvier dernier, sa transposition en droit français nécessite certains ajustements. L'ACPR soutient deux amendements qu'elle juge indispensables pour garantir la cohérence et l'efficacité du dispositif de cyber-résilience.

Le premier concerne l'assujettissement des sociétés de financement. Relevant d'un statut national, elles ne sont en effet pas couvertes par le règlement européen. Cependant, compte tenu de leur rôle crucial dans le secteur bancaire français, il est impératif de leur appliquer les exigences de Dora dans les meilleurs délais. La version adoptée par le Sénat ne prévoit cette application qu'en 2030, ce qui pourrait créer une vulnérabilité pour l'ensemble du secteur financier. À titre d'exemple, Crédit Logement, acteur majeur du crédit immobilier, cautionnait 420 milliards d'euros d'encours en 2024. Or un vol de données personnelles concernant les crédits immobiliers de millions de Français aurait un impact considérable. Face à ce risque, nous préconisons une mise en application rapide du règlement, au moins pour les sociétés de financement les plus critiques. Pour les entités de moindre envergure, nous suggérons une application en janvier 2027, ce qui nous paraît être un délai raisonnable, intervenant deux ans après l'entrée en vigueur du texte.

Concernant l'interaction entre les autorités de contrôle du secteur financier et l'autorité en charge de la cybersécurité dans la gestion des cyberattaques, nous sommes favorables à la mise en place d'une notification parallèle, comme l'autorise le règlement Dora. Cette option permettrait aux établissements d'adresser simultanément leur déclaration d'incident cyber à l'autorité compétente au titre de la directive NIS. Le coût supplémentaire pour les établissements serait nul, puisqu'ils transmettraient les mêmes informations à l'Anssi et à l'ACPR, selon un format identique. En revanche, le gain en termes de stabilité financière serait significatif, chaque heure étant cruciale dans la neutralisation d'une cyberattaque.

L'idée d'une notification unique serait contre-productive, car elle ralentirait le traitement de la menace cyber. Une double notification est au contraire essentielle, car les autorités du secteur financier et l'Anssi ont des missions distinctes. Les unes traitent les conséquences d'un incident cyber pour le secteur financier, notamment la protection de la clientèle, la sauvegarde des avoirs et la gestion du risque systémique, tandis que l'autre se

concentre sur la réponse technique à la cyberattaque. Ce double circuit de notification est donc crucial pour une gestion efficace des incidents.

M. Sébastien Raspiller, **secrétaire général de l'Autorité des marchés financiers (AMF).** Comme l'a souligné Frédéric Hervo, les autorités du secteur financier sont responsables de la mise en œuvre du règlement Dora, dans le respect des compétences respectives de l'ACPR et de l'AMF.

Dora représente un élargissement significatif du périmètre de supervision de l'AMF. Nous sommes en effet désormais chargés de superviser la conformité au règlement des sociétés de gestion, des prestataires de services de financement participatif et des prestataires de services sur actifs numériques. Cette population d'acteurs, nombreuse et majoritairement composée d'entités de petite taille, diffère sensiblement du secteur bancaire et assurantiel. Notre défi majeur consiste à nous assurer de la capacité de ces acteurs à satisfaire les exigences ambitieuses du règlement Dora.

J'ai personnellement participé à la finalisation des négociations du paquet Dora sous la présidence française de l'Union européenne. Le processus législatif au niveau communautaire est pratiquement achevé, avec un seul texte de niveau deux restant à adopter. La mise en œuvre représente maintenant un défi considérable, particulièrement pour les entités de taille modeste.

Notre priorité est d'accompagner ces acteurs, en leur expliquant l'importance cruciale de ces mesures pour réduire la probabilité d'incidents majeurs et en limiter les conséquences. Cela nécessite une montée en compétences significative, non seulement pour l'AMF, mais aussi pour nos homologues européens et les autorités en charge des banques et des assurances. Il s'agit d'un effort collectif, car la résilience globale du système dépend de son maillon le plus faible.

Des exemples récents ont démontré qu'une cyberattaque sur un acteur peut avoir des répercussions en cascade sur de nombreux autres. Il est donc primordial que chaque acteur établisse une cartographie précise de ses vulnérabilités, en tenant compte notamment de l'externalisation croissante des systèmes d'information et d'autres prestations essentielles.

Le règlement Dora introduit également l'obligation de réaliser des tests d'intrusion pour les entités critiques à partir du second semestre. Cela exige de l'AMF l'acquisition de compétences très pointues en matière de cyber-expertise, combinées à une connaissance approfondie des acteurs et des métiers du secteur financier. C'est un véritable défi, car ces compétences sont rares et recherchées, et nous devons rivaliser avec le secteur privé pour attirer ces profils, malgré nos contraintes de service public.

Je tiens à souligner l'aspect très opérationnel de la mise en œuvre de ce règlement qui, s'il est correctement appliqué, devrait significativement renforcer la confiance dans le système financier. Les acteurs conscients des risques pour leur survie, la continuité de leurs activités et leur réputation accueillent favorablement ce cadre visant à améliorer le niveau minimum de résilience parmi les acteurs financiers.

Enfin, je rejoins Frédéric Hervo dans son soutien à la double notification. Bien que le terme « double » puisse suggérer une charge de travail supplémentaire, il s'agit en réalité pour un acteur victime d'une cyberattaque de demander de l'aide simultanément à son superviseur et à l'Anssi. Cette approche ne représente pas une charge significative et garantit une réaction

rapide et efficace. Il est crucial que l'Anssi soit informée directement et rapidement, sans intermédiaire qui pourrait ralentir le processus. Nous apporterons notre expertise spécifique en complément, mais sans entraver la communication directe entre l'entité attaquée et l'Anssi.

M. Éric Bothorel, rapporteur général. Depuis le 17 janvier 2025, comme vous l'avez rappelé, les entités financières sont tenues de notifier les incidents majeurs. Cette obligation concerne les établissements de crédit, les établissements de paiement, les prestataires de services d'information sur les comptes, ainsi que les établissements de monnaie électronique. Ils doivent déclarer les incidents opérationnels ou de sécurité liés aux paiements.

J'aimerais connaître les premiers retours sur cette mise en œuvre. Avez-vous déjà identifié des éléments à modifier ou à améliorer dans le cadre de la loi ?

La Banque de France évalue conjointement avec l'ACPR les vulnérabilités du système financier. Elle œuvre également au renforcement de la résilience et de la sécurité du secteur en veillant à la sécurité et à la robustesse de la place financière. Par ailleurs, la Banque de France contribue à la transformation numérique du secteur en travaillant sur l'euro numérique, la monnaie numérique de banque centrale, et l'infrastructure du marché des capitaux.

Le dernier rapport d'analyse des risques encourus par le système financier souligne que le secteur financier demeure résilient face au risque cyber grâce à ses investissements continus en cybersécurité et sa préparation aux attaques. Néanmoins, de mauvaises pratiques de cybersécurité entraîneraient 2,6 fois plus d'incidents cyber répertoriés et des pertes financières conséquentes, sans compter le risque de réputation et les fuites d'information. Êtes-vous convaincus de l'adéquation du niveau de préparation et de protection actuel ?

Enfin, partagez-vous la position de l'Association de management des risques et des assurances de l'entreprise (Amrae) selon laquelle, pour bénéficier de la couverture d'assurance, il conviendrait de notifier l'incident non pas au moment de sa détection, mais lors de sa présentation à l'assurance ?

M. Mickaël Bouloux, rapporteur. J'ai l'honneur d'être le rapporteur thématique pour le titre III du projet de loi qui porte sur la résilience opérationnelle numérique du secteur financier et transpose la directive Dora du 14 décembre 2022. J'ai noté ce matin, lors de la réunion qui s'est tenue avec la direction générale du Trésor que nous retrouvons des thématiques communes, notamment concernant le formulaire de notification aux entités. J'aurai également l'occasion de rencontrer la Fédération bancaire française en fin de semaine. J'ai bien pris note de vos recommandations concernant les sociétés de financement de type Crédit Logement. Nous avons également discuté avec le Trésor de la question du signalement des incidents. Vous avez déjà abordé la question du double assujettissement entre Dora et NIS 2, du moins pour cette partie relative aux notifications. Si vous identifiez d'autres points de chevauchement, je suis intéressé de les connaître.

Quels obstacles avez-vous pu identifier dans la mise en application du règlement Dora ? Je fais référence à la fois à sa mise en œuvre par les entités financières que vous supervisez, mais aussi par votre propre institution, étant donné que le règlement comporte un certain nombre d'obligations et de changements qui vous concernent également. J'ai bien noté que vous avez évoqué notamment le sujet des ressources humaines et l'accès aux compétences en cybersécurité, un enjeu qui sera largement partagé.

Concernant l'articulation entre la directive et le règlement, pensez-vous que ces deux textes européens sont suffisants pour protéger notre système financier contre les risques liés aux technologies de l'information et de la communication ? Envisagez-vous des étapes supplémentaires ou des améliorations ?

Enfin, quel rôle avez-vous joué lors de l'élaboration de ces textes ? Avez-vous le sentiment d'avoir été écoutés lors des négociations en amont de cette législation européenne ?

Mme Anne Le Hénanff, rapporteure. Pourriez-vous dissiper les inquiétudes exprimées par certains acteurs auditionnés concernant le risque de double assujettissement à NIS 2 et Dora, en particulier au regard de l'article 43A introduit par le sénateur Canevet au Sénat ?

Par ailleurs, il me semble que certains groupes bancaires intègrent désormais la notion de cybersécurité pour leurs propres clients. Votre intervention s'étend-elle jusqu'à ce niveau ? Accompagnez-vous les organismes bancaires dans leur relation avec leurs clients en matière de cybersécurité ? Si c'est le cas, de quelle manière procédez-vous ?

Étant donné que certaines banques ont déjà établi des critères d'exigence en matière de cybersécurité pour leurs clients, ne pensez-vous pas que Dora pourrait agir comme un stimulateur, un moteur, voire une opportunité, ou avoir un effet d'entraînement vis-à-vis du client final ? Je serais très intéressé de connaître votre analyse de l'impact de Dora jusqu'au bout de la chaîne.

Mme Catherine Hervieu, rapporteure. Vous avez évoqué la question des cryptomonnaies et des monnaies numériques. Je souhaiterais apporter quelques précisions en lien avec les développements au sein de l'Eurosystème et le projet d'émission d'une monnaie virtuelle complémentaire aux espèces et aux autres moyens de paiement. Dans cette perspective, l'euro numérique pourrait être déployé à partir de 2027 ou 2028.

Concernant les cryptomonnaies, certains acteurs économiques souhaitent développer leur utilisation, ce qui soulève des questions malgré la mise en application du règlement sur les marchés de crypto-actifs (Mica) par l'Union européenne, visant à assurer la stabilité des entreprises crypto et la protection des consommateurs.

Vous avez souligné dans vos propos introductifs la rapidité exponentielle de la digitalisation, qui nous pose des défis constants. À cet égard, il est important de noter qu'en 2021, 70 % des cyberattaques et des rançongiciels officiellement recensés exigeaient un paiement en cryptomonnaies, dont le célèbre bitcoin pour 60 % d'entre eux.

Dans ce contexte, le travail sur la transposition de la directive européenne pour sécuriser à la fois les infrastructures sensibles et critiques, les aspects financiers et les aspects cyber revêt une importance capitale. En tant que rapporteure pour le titre I^{er}, je suis particulièrement sensible à ces enjeux, d'autant plus que la problématique de fond reste la fragilisation potentielle des États.

Selon vous, quels moyens peuvent être mis en œuvre pour tracer efficacement les attaques, sécuriser l'ensemble du système et mettre en place des mesures de lutte anticipant ces évolutions technologiques qui s'accélèrent de manière exponentielle ?

M. Frédéric Hervo. D'après nos premières expériences en matière d'incidents et de leur notification, il convient de souligner l'apport majeur de Dora. Ce règlement établit un

cadre harmonisé pour le reporting et la notification des incidents, ainsi que pour leur traitement coordonné entre autorités, tant au niveau national qu'européen. Dora prévoit notamment un mécanisme de gestion des incidents majeurs susceptibles d'avoir un impact à l'échelle européenne.

Selon les dispositions de Dora, les incidents majeurs, définis selon des critères spécifiques énoncés dans le règlement, doivent être notifiés aux autorités compétentes dans un délai de quatre heures après leur qualification comme majeurs, et au plus tard vingt-quatre heures après leur survenance. Ce dispositif est entré en vigueur le 17 janvier dernier.

Au 2 juin 2025, l'ACPR a reçu 76 notifications d'incidents majeurs. Ce chiffre, bien que significatif, doit être nuancé pour deux raisons principales. Tout d'abord, un même incident a pu faire l'objet de notifications multiples par plusieurs entités affectées. L'incident Harvest, largement médiatisé et ayant impacté plusieurs entités financières, en est un exemple probant. Ensuite, nous sommes au début de la mise en œuvre de ce dispositif. Certains acteurs ont donc tendance à notifier par précaution, même lorsqu'ils ne sont pas entièrement certains du caractère majeur de l'incident.

Concernant la typologie des incidents signalés, près de la moitié sont liés à des défaillances informatiques opérationnelles, ce qui relève des problématiques classiques de continuité opérationnelle. Un quart concerne des incidents de paiement et un autre quart est d'origine cyber, incluant notamment l'incident Harvest, qui a mis en lumière l'importance cruciale de la chaîne d'externalisation dans la vulnérabilité potentielle des systèmes.

Les premiers retours d'expérience démontrent l'utilité indéniable de ce dispositif de notification, bien que nous soyons encore dans une phase d'apprentissage. Il permet aux autorités d'avoir rapidement une visibilité sur les entités du secteur financier affectées, facilitant ainsi la coordination de la réponse entre les différentes autorités, y compris l'Anssi, et la communication avec les entités impactées.

Ce dispositif ne remplace pas les mécanismes préexistants. Dora vient normaliser et harmoniser ces pratiques, en établissant des attentes claires en termes de délais et de procédures.

Jusqu'à présent, nous n'avons pas eu à traiter d'incident majeur à l'échelle européenne. La plupart de ceux qui ont été signalés ont une portée nationale et sont généralement résolus rapidement, en particulier quand ils sont liés à la continuité opérationnelle. Bien que nous soyons toujours en phase d'apprentissage, Dora démontre déjà toute son utilité dans la gestion et la coordination des incidents au sein du secteur financier.

M. Sébastien Raspiller. Pour compléter ces informations du point de vue de l'AMF, nous avons reçu une trentaine de notifications depuis la mise en œuvre de Dora mi-janvier. La répartition est la suivante : 40 % concernent des cyberattaques, environ la moitié sont liées à des problèmes de disponibilité des services informatiques et 10 % relèvent de pannes basiques.

Le nombre de notifications est relativement significatif, d'autant plus que nous avons observé un temps d'adaptation nécessaire pour les acteurs, particulièrement ceux de plus petite taille, afin qu'ils comprennent et appliquent correctement les nouvelles exigences de notification standardisée. Nous constatons une amélioration progressive : les notifications arrivent désormais dans les délais impartis et respectent le format requis. Bien que

l'apprentissage soit toujours en cours, nous notons une amélioration sensible. Les acteurs semblent également avoir intégré qu'il est préférable de notifier de manière prudente plutôt que d'attendre d'être absolument certains de la nécessité de le faire.

M. Frédéric Hervo. Concernant l'état de préparation de la place financière, et selon la perception que nous pouvons avoir de l'ensemble de la chaîne, il est important de souligner la maturité relative du secteur financier en matière de cybersécurité. Elle s'explique notamment par le fait que ce secteur figure parmi les plus ciblés par les cyberattaques, ce qui a conduit à une sensibilisation accrue depuis longtemps.

Dora apporte une approche homogène pour l'ensemble du secteur financier, unifiant des réglementations qui étaient auparavant sectorielles. Cependant, nous ne partons pas de zéro. Le premier pilier de Dora, qui concerne l'analyse des risques propres à chaque institution, l'identification de ses vulnérabilités, la mise en place de différents niveaux de contrôle et l'implication de la gouvernance, s'appuie sur des concepts déjà bien établis.

L'aspect le plus novateur de Dora, qui nécessitera un travail important de la part des acteurs cette année, concerne l'introduction de clauses-types obligatoires dans les contrats d'externalisation avec les prestataires critiques. Cet élément est crucial, notamment dans le contexte de l'utilisation croissante des services de *cloud computing*, où le pouvoir de négociation des établissements financiers face aux géants technologiques était souvent limité. Ces clauses standardisées renforcent la position des acteurs du secteur financier vis-à-vis de ces prestataires, souvent extérieurs à l'Union européenne.

Notre rôle en tant qu'autorités a été essentiel dans la sensibilisation à ces nouvelles dispositions. Nous avons organisé de nombreuses réunions avec les associations professionnelles pour expliquer les implications de Dora, notamment en ce qui concerne les tests d'intrusion. Dora exige en effet que les entités mettent en place leur propre plan de tests d'intrusion à terme, ce qui représente un changement significatif dans leurs pratiques de cybersécurité.

Le principe de proportionnalité s'applique à l'ensemble des acteurs soumis à Dora. Pour un sous-ensemble plus restreint d'entités critiques ou systémiques, des tests sous le contrôle des autorités de supervision seront mis en place. Ces tests visent à détecter les points de vulnérabilité dans les systèmes critiques pour les services financiers, à l'instar d'un hacker externe.

Nous commencerons à déployer ce dispositif très exigeant en termes d'expertise et de ressources à partir du second semestre, sur un cycle triennal. Il est évident que les plus petits acteurs ou certains secteurs, notamment l'assurance et les mutuelles, plus dispersés, partent de plus loin en termes de sensibilisation. Notre approche sera progressive, pragmatique et proportionnée, privilégiant l'accompagnement avant le contrôle.

Concernant les clients, nous constatons des liens importants avec la fraude, particulièrement celle liée aux paiements. Il est crucial de rappeler les bonnes pratiques de prévention à la clientèle, d'autant plus que l'évolution technologique, notamment l'utilisation de l'intelligence artificielle, facilite certains dispositifs frauduleux.

Dora souligne à juste titre l'importance d'une prise en compte rigoureuse de toute la chaîne des prestataires externes dans le cadre de l'externalisation. L'incident Harvest illustre parfaitement cette nécessité : la cyberattaque qui a affecté ce fournisseur de logiciels pour de

nombreux acteurs, dont des conseillers en gestion de patrimoine, provenait en réalité d'un de ses propres prestataires. Cet exemple démontre l'importance de considérer l'intégralité de la chaîne de sous-traitance et d'externalisation.

Dora représente indéniablement une avancée significative. Cependant, les menaces continuent d'évoluer, et il est impératif de réduire l'avance des organisations criminelles ou para-étatiques. Une évaluation de Dora sera nécessaire après quelques années d'application.

Concernant l'articulation entre NIS 2 et Dora, deux points méritent d'être soulignés. Tout d'abord, Dora étant un texte spécialisé, une entité du secteur financier répondant à ses exigences n'est pas soumise à NIS 2, ce qui constitue une simplification. Ensuite, la double notification des incidents est une nécessité opérationnelle. Bien que nous partagions les notifications reçues avec diverses autorités, y compris au niveau européen, il est crucial que l'Anssi, en tant qu'autorité responsable, reçoive directement ces notifications, même si cela implique un doublon. Cette approche nous permet de gagner un temps précieux dans la réponse aux incidents, sans remettre en cause le principe général selon lequel NIS 2 ne s'applique pas au secteur financier, Dora étant la loi spéciale en la matière.

M. Sébastien Raspiller. L'AMF est chargée de l'agrément des prestataires de services sur actifs numériques et assumera également la supervision de ces acteurs dans le cadre de Dora. Ces entités, déjà familiarisées avec certaines exigences grâce au régime national issu de la loi Pacte, sont souvent des acteurs conséquents et intrinsèquement digitaux, opérant à l'échelle européenne et internationale.

Nous avons récemment observé des incidents majeurs de vol de données et de cryptoactifs, comme celui survenu en février sur une plateforme internationale, impliquant 1,6 milliard de dollars. Il est à noter que cette plateforme n'était pas autorisée à opérer en France, n'étant pas enregistrée conformément à la loi Pacte. Notre vigilance a permis d'éviter que des clients français ne soient affectés par ce piratage.

Bien que le règlement Mica n'ait pas retenu l'obligation d'un audit cyber réalisé par un prestataire certifié, contrairement à ce que prévoyait la loi Pacte, nous encourageons vivement les acteurs à maintenir cette pratique. De nombreux opérateurs le font spontanément, conscients de l'importance de cette démarche pour la confiance de leurs clients.

Les prestataires de services sur actifs numériques sont pleinement intégrés dans le champ d'application de Dora, avec une exposition particulièrement élevée aux risques de cyberattaques. Nous observons généralement une bonne maturité chez ces acteurs en France, mais ce niveau peut varier à travers l'Union européenne et au-delà. Le passeport européen prévu par le règlement Mica rend d'autant plus crucial le renforcement des exigences en matière de cybersécurité au niveau européen.

Concernant l'articulation entre NIS 2 et Dora, nous saluons la mise en place d'un point d'entrée unique pour les autorités de supervision financière, ce qui simplifie les procédures et évite les doublons. Cette approche est particulièrement pertinente pour les acteurs sous supervision conjointe, comme certaines infrastructures de marché supervisées à la fois par la Banque de France et l'AMF.

Quant à l'efficacité de Dora, il est prématuré d'envisager une version ultérieure. L'objectif n'est pas d'atteindre un monde sans cyberattaques, ce qui est irréaliste, mais de

réduire significativement leur occurrence et leurs impacts. Le succès de Dora se mesurera à sa capacité à améliorer les investissements en cybersécurité et à atténuer les effets des attaques lorsqu'elles surviennent.

La résilience est un enjeu crucial pour toute entité consciente des risques cybernétiques. Il s'agit non seulement de savoir y faire face lorsqu'ils surviennent, mais aussi de s'efforcer d'en réduire la fréquence. C'est à l'aune de ces critères que nous pourrons juger de l'efficacité de Dora, bien qu'il soit encore trop tôt pour tirer des conclusions définitives.

Concernant les obstacles, j'ai évoqué précédemment les défis liés aux ressources humaines. Au-delà du recrutement de cyber-experts, nous devons impérativement élever le niveau de compétence de l'ensemble des acteurs impliqués dans la supervision classique. Cette exigence s'applique tant à notre personnel qu'aux gestionnaires externes. Le risque cyber n'étant pas nécessairement leur préoccupation première, il est essentiel qu'ils intègrent pleinement les enjeux de Dora dans leurs pratiques. Cela implique un effort considérable en matière de formation.

À titre d'exemple, nous avons récemment organisé une journée dédiée aux enjeux de Dora pour les équipes de conformité et de contrôle interne, rassemblant 450 participants. Nous proposons également des webinaires d'accompagnement. Notre objectif est de rendre ces informations accessibles non seulement aux cyber-experts, mais aussi à un public plus large dont ce n'est pas le cœur de métier. C'est un véritable défi que nous devons relever.

Un autre enjeu majeur concerne la mise en place des couches nationales prévues par Dora. Bien que nous bénéficiions d'une excellente coordination avec l'autorité nationale, la dimension européenne ajoute un niveau de complexité. Les trois autorités européennes de supervision devront se coordonner efficacement, ce qui représente une nouveauté potentiellement source de difficultés. Il sera crucial de s'assurer du bon fonctionnement de cette collaboration.

Quant à savoir si l'Autorité a été écoutée lors de l'élaboration de Dora, je peux témoigner, pour avoir été de l'autre côté, que j'ai consacré un temps considérable à l'écoute des dix autorités concernées. J'ose espérer qu'elles ont été non seulement entendues, mais aussi écoutées. Cependant, il leur appartiendra d'en juger.

Le débat le plus ardu a porté sur les fournisseurs de cloud et la possibilité d'une extra-territorialité. Mais la question ne se limite pas à ce seul aspect. D'autres fournisseurs de données, par exemple, peuvent également avoir un impact systémique considérable. Prenons le cas de la gestion d'actifs basée sur des indices : une erreur dans le calcul de ces indices pourrait avoir des conséquences désastreuses pour les clients et les épargnants.

J'ai observé une évolution dans l'attitude des prestataires tiers critiques. Alors qu'ils exerçaient un lobbying intense lors des négociations politiques initiales, ils semblent aujourd'hui avoir accepté l'inévitabilité de leur inclusion dans le périmètre de Dora. Ils demandent désormais des clarifications pour se mettre en conformité, ce qui témoigne d'une compréhension accrue des bénéfices potentiels de cette réglementation, notamment en termes de justification des investissements nécessaires en interne.

En conclusion, au-delà des obstacles identifiés, ces évolutions constituent des facteurs de réussite potentiels pour la mise en œuvre efficace de Dora.

M. le président Philippe Latombe. Des questions se posent quant à l'articulation le règlement général de protection des données personnelles (RGPD), la Commission nationale informatique et libertés (CNIL) et Dora. Si l'architecture entre NIS 2 et la CNIL est clairement définie, qu'en est-il de la relation entre Dora et la CNIL ? En tant qu'autorité de référence pour le secteur financier, comment gérez-vous les incidents cybernétiques ayant un impact sur les données personnelles ? Existe-t-il une coordination particulière avec la CNIL dans ces situations ?

Mme Laetitia Saint-Paul (HOR). Vous avez indiqué que l'intelligence artificielle (IA) facilitait les dispositifs de fraude. Pourriez-vous nous éclairer sur la manière dont les cybercriminels exploitent concrètement l'IA ? Par ailleurs, comment l'utilisez-vous de votre côté à des fins défensives, sachant que les criminels ont souvent une longueur d'avance ?

Pouvez-vous préciser dans quelle mesure les cryptomonnaies facilitent ou non le blanchiment d'argent ? Face à l'adage « suivez l'argent » souvent cité en matière de criminalité, quels sont les nouveaux moyens développés pour contrer ce blanchiment, notamment dans le contexte des cryptomonnaies ?

Enfin, vous avez indiqué que 70 % des cyberattaques étaient des attaques par rançongiciel. Pourriez-vous détailler la répartition des 30 % restants ?

M. Sébastien Raspiller. Concernant l'articulation entre Dora et le RGPD, notre rôle de superviseur nous amène à vérifier que les entités assujetties respectent l'ensemble des réglementations applicables. Ainsi, lorsqu'une fuite de données personnelles est signalée dans le cadre de Dora, nous nous assurons que l'entité a bien effectué les déclarations nécessaires auprès de la CNIL, conformément au RGPD. Cette procédure est désormais bien intégrée dans les pratiques des entités supervisées. À ce jour, nous n'avons pas identifié de difficultés majeures dans cette articulation entre Dora et le RGPD. Si des problèmes devaient survenir, ils seraient traités dans le cadre de notre dialogue de supervision.

Concernant l'utilisation de l'IA dans les fraudes, nous observons effectivement une recrudescence inquiétante. Selon les études de l'AMF, 15 % des Français estiment avoir été victimes ou cibles d'une tentative d'arnaque financière, ce chiffre atteignant 35 % chez les moins de 35 ans. Bien que le nombre d'arnaques effectives soit inférieur, la tendance est préoccupante avec une multiplication par trois sur les trois dernières années.

Parmi ces fraudes, certaines exploitent déjà l'intelligence artificielle, notamment à travers l'utilisation de *deepfakes*. Ces techniques permettent de manipuler l'image et la voix de personnalités connues pour leur faire tenir des propos qu'elles n'ont jamais prononcés, créant ainsi des publicités trompeuses mettant en scène des journalistes, des hommes politiques ou des célébrités du sport.

Face à cette menace croissante, notre action se déploie sur plusieurs fronts. Nous multiplions les alertes pour sensibiliser le public et nous transmettons systématiquement les cas détectés aux autorités judiciaires compétentes. Néanmoins, nous sommes conscients que le développement de l'IA continuera d'amplifier ce phénomène, nécessitant une vigilance accrue et des moyens de lutte toujours plus sophistiqués.

Bien que l'imitation ne soit pas encore parfaite, les progrès rapides accomplis pour générer des avatars laissent présager une amélioration significative de la qualité dans un avenir proche. Nous travaillons activement sur l'utilisation de l'IA pour nous protéger contre

ces technologies de manipulation. Il est vrai que le secteur privé a souvent une longueur d'avance, mais je ne peux pas totalement abonder dans votre sens en tant que superviseur.

Il est indéniable que la lutte contre ces technologies représente un défi majeur. Les autorités doivent impérativement investir dans des moyens de détection adéquats pour ne pas se laisser distancer. Parallèlement, des mesures plus basiques s'avèrent essentielles. Nous avons ainsi lancé une campagne d'éducation financière axée sur un principe fondamental : il n'est jamais urgent de perdre de l'argent. L'objectif est d'inciter à la prudence face aux offres alléchantes assorties de délais artificiellement courts. Ces réflexes élémentaires doivent être constamment rappelés.

La technologie jouera un rôle crucial dans la lutte contre des manipulations de plus en plus sophistiquées, mais elle doit s'accompagner d'approches préventives et éducatives. Concernant les cryptoactifs, l'AMF a hérité de compétences élargies, notamment en matière de lutte contre le blanchiment, conformément à la loi Pacte. Si la traçabilité inhérente à la blockchain est un atout, l'enjeu principal réside dans l'identification des utilisateurs. Le règlement européen révisé sur les transferts de fonds (TFR), entré en vigueur récemment, impose désormais l'identification réelle des parties lors des transferts de cryptoactifs, à l'instar des règles appliquées aux transferts de fonds traditionnels. Cette réglementation vise à garantir une transparence comparable entre les transactions en cryptoactifs et celles en monnaie fiduciaire.

Je souscris pleinement aux propos de Sébastien Raspiller concernant les cryptoactifs et leur vulnérabilité face aux risques de blanchiment. Le règlement Mica, en instaurant un cadre réglementaire pour certaines activités liées aux cryptoactifs, y compris sous l'angle de la lutte contre le blanchiment et le financement du terrorisme, permet de mettre en place un dispositif de contrôle efficace. Bien que ce règlement ne couvre pas l'intégralité du secteur, notamment la finance décentralisée, il constitue une avancée significative.

Concernant l'intelligence artificielle, je souhaite évoquer un autre exemple d'utilisation frauduleuse : la modernisation de la fraude au président. Cette escroquerie classique, où un imposteur se fait passer pour un dirigeant d'entreprise afin d'obtenir un virement urgent, se voit aujourd'hui amplifiée par l'IA. Les fraudeurs exploitent désormais les réseaux sociaux et les techniques d'imitation vocale pour rendre leurs tentatives plus crédibles.

L'IA, comme toute évolution technologique, offre de nouvelles opportunités aux fraudeurs, mais également de nouvelles perspectives pour la lutte anti-fraude. À titre d'exemple, de nombreux établissements financiers commencent à utiliser massivement l'IA pour analyser les flux d'opérations dans le cadre de la lutte contre le blanchiment et le financement du terrorisme (LCB-FT). Ces outils permettent un criblage plus efficace des opérations sensibles et facilitent la préparation des déclarations de soupçon. Certains grands groupes financiers ont déjà mis en œuvre ces technologies, tandis que d'autres en sont encore au stade de l'expérimentation. L'ACPR, qui joue un rôle prépondérant dans la prévention du blanchiment et du financement du terrorisme, évalue actuellement ces évolutions intéressantes sur le principe.

La séance est levée à 17 heures 45

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 3 juin 2025 à 16 h 35

Présents. - M. Éric Bothorel, M. Mickaël Bouloux, Mme Virginie Duby-Muller, Mme Catherine Hervieu, M. Philippe Latombe, Mme Anne Le Hénanff, Mme Élisabeth de Maistre, M. Stéphane Rambaud, Mme Marie Récalde, Mme Laetitia Saint-Paul, M. Vincent Thiébaut, Mme Sabine Thillaye

Excusé. - M. Laurent Mazaury