ASSEMBLÉE NATIONALE

5 septembre 2025

RÉSILIENCE DES INFRASTRUCTURES CRITIQUES ET RENFORCEMENT DE LA CYBERSÉCURITÉ - (N° 1112)

Tombé

N° CS109

AMENDEMENT

présenté par
M. Latombe

ARTICLE 43 A

Rédiger ainsi cet article :

« I. - Après l'article L. 612-24 du code monétaire et financier, il est inséré un article L. 612-24-1 ainsi rédigé :

« *Art. L. 612-24-1*. – I. – En application du premier alinéa du paragraphe 1 de l'article 19 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, les entités financières soumises à ce règlement qui relèvent de la compétence de l'Autorité de contrôle prudentiel et de résolution, à l'exception des personnes mentionnées au *b* du 2° du A du I de l'article L. 612-2, adressent à l'Autorité de contrôle prudentiel et de résolution leurs déclarations d'incidents majeurs liés aux technologies de l'information et de la communication.

« Lorsque ces entités sont également soumises en tant qu'entités essentielles ou importantes aux dispositions de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, elles transmettent également à l'autorité nationale de sécurité des systèmes d'information, en application du sixième alinéa du 1 de l'article 19 du règlement mentionné à l'alinéa précédent, leurs déclarations d'incidents majeurs liés aux technologies de l'information et de la communication.

« II. – En application du paragraphe 2 de l'article 19 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, les entités financières mentionnées au premier alinéa du I peuvent adresser à l'Autorité de contrôle prudentiel et de résolution leurs notifications de cybermenaces. Dans ce cas, elles transmettent également ces notifications à l'autorité nationale de sécurité des systèmes d'information.

« III. – Les déclarations et notifications mentionnées au I et au II du présent article sont réalisées

par le biais d'un document unique transmis simultanément à l'Autorité de contrôle prudentiel et de résolution et à l'autorité nationale de sécurité des systèmes d'information. »

« II. – Au tableau du I des articles L. 783-2, L. 784-2 et L. 785-2 du même code, après la ligne :

«

L. 612-24, à l'exception de son huitième alinéa	l'ordonnance n° 2021-796 du 23 juin 2021

»

est insérée la ligne suivante :

«

L. 612-24-1	la loi n° du 2025

».

EXPOSÉ SOMMAIRE

Cet amendement vise à désigner l'Autorité de contrôle prudentiel et de résolution comme autorité compétente chargée de recevoir les déclarations d'incidents majeurs liés aux TIC et les notifications volontaires des cybermenaces de la part des entités financières soumises à la surveillance de plusieurs autorités nationales compétentes, conformément au deuxième alinéa du paragraphe 1 de l'article 19 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (DORA).

Contrairement à la rédaction adoptée par le Sénat, une communication simultanée et par le biais d'un formulaire unique est toutefois prévue au bénéfice de l'Agence nationale de sécurité des systèmes d'information (ANSSI), de manière obligatoire pour les entités assujetties au titre II du projet de loi et sur une base volontaire pour les autres entités, afin de faciliter l'information rapide et le traitement de ces incidents et menaces par l'ANSSI.

Cette rédaction permet de concilier la simplification des démarches à accomplir par les entreprises concernées tout en permettant l'intervention rapide de l'ANSSI.

En effet, une transmission à la seule ACPR engendrerait des délais importants, notamment en cas d'incidents nocturnes ou le week-end, l'ACPR ne disposant ni d'un système d'astreinte ni d'un portail de déclaration accessible en continu, contrairement à l'ANSSI. Ces délais peuvent être très préjudiciables dans le cadre de la gestion d'incidents cyber majeurs. Certains incidents peuvent affecter directement la situation prudentielle d'un établissement ou perturber la continuité de ses services essentiels. Dans ce contexte, une information directe et simultanée des autorités financières est indispensable pour permettre une réaction rapide, prévenir tout risque de contagion et sécuriser les intérêts des clients.