Finance numérique: loi sur la résilience opérationnelle numérique (DORA)

2020/0266(COD) - 24/09/2020 - Document de base législatif

OBJECTIF : définir des exigences uniformes concernant la sécurité des réseaux et des systèmes d'information qui soutiennent les processus opérationnels des entités financières en vue d'atteindre un niveau élevé de résilience numérique opérationnelle pour le secteur financier.

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : la présente proposition s'inscrit dans un nouvel ensemble de mesures sur la finance numérique visant à soutenir davantage le potentiel du financement numérique en termes d'innovation et de concurrence tout en atténuant les risques.

Le paquet sur le « financement numérique » comprend une nouvelle stratégie sur le financement numérique qui vise à garantir que la législation de l'Union sur les services financiers est adaptée à l'ère numérique et contribue à une économie tournée vers l'avenir en rendant l'utilisation de technologies innovantes plus accessible aux consommateurs et aux entreprises européennes. Il est de l'intérêt politique de l'Union de développer et de promouvoir l'adoption de technologies de transformation numérique dans le secteur financier, y compris la technologie des chaînes de blocs et des registres distribués (DLT).

Ce paquet comprend également une proposition de règlement visant à établir un nouveau cadre juridique européen en vue d'assurer le bon fonctionnement des marchés des crypto-actifs, une proposition de règlement sur un régime pilote pour les infrastructures de marché basé sur la technologie des registres distribués (DLT) et une proposition visant à clarifier ou à modifier certaines règles communautaires connexes en matière de services financiers.

Au cours des dernières décennies, l'utilisation des technologies de l'information et de la communication (TIC), a joué un rôle central dans la finance, et revêt aujourd'hui une importance cruciale dans le fonctionnement quotidien de toutes les entités financières. La numérisation couvre, par exemple, les paiements, qui sont de plus en plus passés de méthodes basées sur l'argent liquide et le papier à l'utilisation de solutions numériques. La finance est devenue largement numérique dans l'ensemble du secteur.

Cependant, l'accroissement de la numérisation et de l'interconnexion amplifie également les risques liés aux TIC, ce qui rend la société dans son ensemble - et le système financier en particulier - plus vulnérable aux cybermenaces.

Les risques liés aux TIC posent des défis pour les performances et la stabilité du système financier de l'UE. L'absence de règles détaillées et complètes sur la résilience opérationnelle numérique au niveau de l'UE a conduit à la prolifération d'initiatives réglementaires nationales (par exemple, en ce qui concerne les tests de résilience opérationnelle numérique) et d'approches de surveillance (par exemple, en ce qui concerne la dépendance à l'égard des fournisseurs d'infrastructures et de services tiers).

Cette situation fragmente le marché unique, porte atteinte à la stabilité et à l'intégrité du secteur financier de l'UE et compromet la protection des consommateurs et des investisseurs. La Commission estime donc

nécessaire de mettre en place un cadre détaillé et complet sur la résilience opérationnelle numérique pour les entités financières de l'UE.

CONTENU : la proposition vise à mettre en place un cadre global qui améliorera la gestion des risques liés au numérique. En particulier, elle vise à renforcer et à rationaliser la conduite de la gestion des risques liés aux TIC par les entités financières, à imposer à toutes les entreprises de veiller à pouvoir résister à tous les types de perturbations et de menaces liées à l'informatique, à sensibiliser les superviseurs aux cyber-risques et aux incidents liés aux TIC auxquels sont confrontées les entités financières, ainsi qu'à introduire des pouvoirs permettant aux superviseurs financiers de surveiller les risques découlant de la dépendance des entités financières à l'égard des tiers fournisseurs de services TIC, tels que les prestataires de services d'informatique en nuage.

Champ d'application du règlement

Afin d'assurer la cohérence des exigences de gestion des risques liés aux TIC applicables au secteur financier, le règlement proposé couvrira une série d'entités financières réglementées au niveau de l'Union, à savoir, entre autres : i) les banques, ii) les établissements de paiement, iii) les établissements de monnaie électronique, iv) les entreprises d'investissement, les fournisseurs de services de cryptage, v) les dépositaires centraux de titres, vi) les contreparties centrales, vii) les bourses, viii) les référentiels centraux, ix) les agences de notation du crédit.

Une telle couverture devrait faciliter une application homogène et cohérente de tous les éléments de la gestion des risques dans les domaines liés aux TIC, tout en préservant l'égalité des conditions de concurrence entre les entités financières en ce qui concerne leurs obligations réglementaires en matière de risques liés aux TIC.

Exigences liées à la gouvernance

Dans la mesure où la proposition vise à mieux aligner les stratégies commerciales des entités financières et la conduite de la gestion des risques liés aux TIC, l'organe de direction devrait conserver un rôle crucial et actif dans le pilotage du cadre de gestion des risques liés aux TIC et veiller au respect d'une cyberhygiène rigoureuse.

Exigences en matière de gestion des risques liés aux TIC

La résilience opérationnelle numérique est ancrée dans un ensemble de principes et d'exigences clés sur le cadre de gestion des risques liés aux TIC, conformément aux conseils techniques conjoints des Autorités européennes de surveillance (AES). Ces exigences, inspirées des normes, lignes directrices et recommandations internationales, nationales et sectorielles pertinentes, tournent autour de fonctions spécifiques de la gestion des risques liés aux TIC (identification, protection et prévention, détection, réponse, apprentissage, évolution et communication).

Pour suivre l'évolution rapide du paysage des cybermenaces, les entités financières seraient tenues de mettre en place et de maintenir des systèmes et des outils TIC résilients qui minimisent l'impact des risques liés aux TIC.

Rapports d'incidents liés aux TIC

La proposition crée un mécanisme cohérent de notification des incidents qui contribuera à réduire les charges administratives des entités financières et à renforcer l'efficacité de la surveillance. La déclaration serait traitée à l'aide d'un modèle commun et selon une procédure harmonisée, telle que mise au point par les AES.

Test de résilience opérationnelle numérique

Les capacités et les fonctions incluses dans le cadre de gestion des risques liés aux TIC devraient être testées périodiquement pour vérifier l'état de préparation et identifier les faiblesses, les déficiences ou les lacunes, ainsi que pour mettre en œuvre rapidement des mesures correctives. La proposition permet une application proportionnée des exigences de test de résilience opérationnelle numérique en fonction de la taille, de l'activité et des profils de risque des entités financières.

Partage d'informations

Afin de sensibiliser au risque lié aux TIC, de minimiser sa propagation, de soutenir les capacités défensives des entités financières et les techniques de détection des menaces, le règlement proposé permet aux entités financières de mettre en place des arrangements pour échanger entre elles des informations et des renseignements sur la cybermenace. Tous les accords volontaires d'échange d'informations entre entités financières que la proposition encourage seraient menés dans des environnements de confiance, dans le respect total des règles de l'Union en matière de protection des données.

Implications budgétaires

Dès lors que le règlement prévoit un rôle accru pour les AES pour surveiller de manière adéquate les fournisseurs tiers de TIC critiques, la proposition impliquerait le déploiement de ressources accrues, notamment pour remplir les missions de surveillance (telles que les inspections et les audits sur site et en ligne) et le recours à du personnel possédant une expertise spécifique en matière de sécurité des TIC.

L'ampleur et la répartition de ces coûts dépendront de l'étendue des nouveaux pouvoirs de surveillance et des tâches (précises) à accomplir par les AES.

L'impact total des coûts est estimé à environ 30,19 millions d'euros pour la période 2022 - 2027. Par conséquent, aucune incidence sur les crédits du budget de l'UE n'est prévue (à l'exception du personnel supplémentaire), car ces coûts seront entièrement financés par les redevances.