Finance numérique: directive modifiant sur les exigences en matière de résilience opérationnelle numérique

2020/0268(COD) - 07/12/2021 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission des affaires économiques et monétaires a adopté le rapport de Mikuláš PEKSA (Verts /ALE, CZ) sur la proposition de directive du Parlement européen et du Conseil modifiant les directives 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341.

La présente proposition législative fait partie du train de mesures sur la finance numérique. Elle introduit :

- des modifications ciblées aux directives existantes de l'Union portant sur les services financiers afin de les aligner sur les exigences établies par le règlement sur la résilience opérationnelle numérique du secteur financier (règlement DORA) en matière de gestion des risques et de notification s'agissant de l' informatique et des réseaux et systèmes d'information, et de clarifier certaines dispositions pour garantir une pleine prise en compte des risques informatiques;

- des modifications ciblées de la directive concernant les marchés d'instruments financiers (MiFID) afin d' apporter une sécurité juridique en ce qui concerne la définition des crypto-actifs et de créer une exemption temporaire permettant aux personnes physiques de participer, sous certaines conditions, au régime pilote pour un système multilatéral de négociation DLT (technologie des registres distribués).

La commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Exigences liées au risque informatique

Les dispositions existantes du droit de l'Union n'étant pas totalement harmonisées, les députés insistent sur la nécessité d'éviter une réglementation excessive et de garantir l'adéquation de ces dispositions à la réalité qui évolue constamment dans ce domaine. Il s'agit également de garantir le bon fonctionnement du marché intérieur tout en encourageant la **proportionnalité**, notamment en ce qui concerne les PME, les autres petites entités financières et les autres microentreprises, dans le but de réduire les coûts de mise en conformité.

Modification de la directive 2013/36/UE concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement (CRD)

Les dispositions pertinentes de la CRD ont été clarifiées de manière à ce que le risque informatique soit explicitement pris en compte.

Les modifications introduites stipulent que les établissements doivent disposer d'un **dispositif solide de gouvernance d'entreprise**, comprenant notamment i) une structure organisationnelle claire avec un partage des responsabilités bien défini, transparent et cohérent, ii) des processus efficaces de détection, de gestion, de suivi et de déclaration des risques auxquels ils sont ou pourraient être exposés, iii) des mécanismes adéquats de contrôle interne, y compris des procédures administratives et comptables saines, des systèmes de réseau et des systèmes d'information mis en place et gérés conformément au règlement DORA et des politiques et pratiques de rémunération permettant une gestion saine et efficace des risques.

Les établissements devraient mettre en œuvre des mesures et des procédures pour **identifier, évaluer et gérer leurs expositions au risque opérationnel**, y compris le risque découlant de la sous-traitance de fonctions et le risque lié aux tiers prestataires de services informatiques au sens du règlement DORA et pour couvrir les événements qui engendrent de graves répercussions.

En outre, les établissements devraient disposer de plans d'urgence et de poursuite de l'activité adéquats, y compris des stratégies de continuité des activités informatiques et des plans de reprise après sinistre établis, gérés et testés afin qu'ils puissent poursuivre leurs activités en cas de grave perturbation de celles-ci.

Modification de la directive 2014/59/UE établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement (BRRD)

Les risques informatiques et les vulnérabilités en matière de résilience opérationnelle numérique peuvent affecter les réseaux et systèmes d'information qui soutiennent les fonctions critiques des banques et compromettre les objectifs de la résolution. Il est également essentiel de choisir les contrats de services informatiques adéquats pour assurer la continuité opérationnelle et fournir les données nécessaires en cas de résolution.

Afin de respecter les objectifs du cadre européen en matière de résilience opérationnelle, il est proposé de modifier la directive 2014/59/UE pour assurer la prise en compte des informations relatives à la résilience opérationnelle pour planifier la résolution et évaluer la résolvabilité des établissements.

Modification de la directive (UE) 2015/849 (prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou de financement du terrorisme)

Le texte amendé souligne la nécessité garantir la résilience opérationnelle pour renforcer la capacité des établissements financiers à lutter contre le blanchiment de capitaux et le financement du terrorisme, compte tenu notamment des risques croissants et émergents dans ce domaine dans l'environnement post-COVID, où il est devenu plus facile pour les criminels d'exploiter les faiblesses et les lacunes des systèmes et contrôles des établissements.

Par conséquent, il est proposé de modifier la directive (UE) 2015/849 de manière à inclure explicitement, en ce qui concerne les entités soumises à obligations qui relèvent du champ d'application du règlement DORA, les exigences en matière de résilience opérationnelle numérique dans le cadre des politiques, contrôles et procédures mis en place par ces entités soumises à obligations afin d'atténuer et de gérer efficacement les risques de blanchiment de capitaux et de financement du terrorisme.

Modification de directive (UE) 2015/2366 (services de paiement)

La directive énonce des règles spécifiques sur les mesures de maîtrise et d'atténuation des risques en matière de sécurité informatique aux fins d'un agrément pour fournir des services de paiement. Les députés proposent de modifier ces règles d'agrément afin qu'elles soient alignées sur le règlement DORA.

En outre, afin de réduire la charge administrative et d'éviter la complexité et la duplication des obligations de signalement, les règles relatives à la notification des incidents contenues dans ladite directive ne devraient pas s'appliquer aux prestataires de services de paiement qui relèvent du champ d'application du chapitre III du règlement DORA (gestion, classification et notification des incidents liés à l'informatique), ce qui permettra de créer un mécanisme unique, pleinement harmonisé, de signalement des incidents pour les prestataires de services de paiement, applicable à tous les incidents opérationnels ou de sécurité liés à des paiements ou à des non-paiements.