Luxembourg, le 23 octobre 2023

Objet : Projet de loi n°8291[1] portant :

1. **mise en œuvre du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n°600/2014, (UE) n° 909/2014 et (UE) 2016/1011 ;**
2. **transposition de la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier ;**
3. **modification de :**
   a) **la loi modifiée du 5 avril 1993 relative au secteur financier ;**
   b) **la loi modifiée du 13 juillet 2005 relative aux institutions de retraite professionnelle sous forme de sepcav et assep ;**
   c) **la loi modifiée du 10 novembre 2009 relative aux services de paiement ;**
   d) **la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif ;**
   e) **la loi modifiée du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs ;**
   f) **la loi modifiée du 7 décembre 2015 sur le secteur des assurances ;**
   g) **la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement ;**
   h) **la loi modifiée du 30 mai 2018 relative aux marchés d'instruments financiers ;**
   i) **la loi modifiée du 16 juillet 2019 relative à l'opérationnalisation de règlements européens dans le domaine des services financiers. (6475GKA)**

Saisine : Ministre des Finances
(4 août 2023)

Avis de la Chambre de Commerce

Le projet de loi sous avis (ci-après le « Projet ») a deux objectifs :

premièrement, il vise à mettre en œuvre les dispositions du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n°1060/2009, (UE) n°648/2012, (UE) n°600/2014, (UE) n°909/2014 et (UE) n°2016/1011 (ci-après le « Règlement 2022/2554 ») ;

deuxièmement, le Projet a pour objet de transposer en droit luxembourgeois la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier (ci-après la « Directive 2022/2556 »), qui accompagne le Règlement 2022/2554.

[1] Lien vers le texte du projet de loi n°8291 sur le site de la Chambre des Députés

Afin de mettre en œuvre le Règlement 2022/2554 et de transposer la Directive 2022/2556, le Projet procède à la modification de nombreuses lois sectorielles régissant le secteur financier, à savoir (i) la loi modifiée du 5 avril 1993 relative au secteur financier, (ii) la loi modifiée du 13 juillet 2005 relative aux institutions de retraite professionnelle sous forme de sepcav et assep, (iii) la loi modifiée du 10 novembre 2009 relative aux services de paiement, (iv) la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif, (v) la loi modifiée du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs, (vi) la loi modifiée du 7 décembre 2015 sur le secteur des assurances, (vii) la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement, (viii) la loi modifiée du 30 mai 2018 relative aux marchés d'instruments financiers et (ix) la loi modifiée du 16 juillet 2019 relative à l'opérationnalisation de règlements européens dans le domaine des services financiers.

En bref

- La Chambre de Commerce prend note des dispositions du Projet qui mettent en œuvre le Règlement 2022/2554 et transposent la Directive 2022/2556, ces derniers visant à harmoniser et à renforcer les exigences en matière des TIC pour atteindre un niveau élevé de résilience opérationnelle numérique pour l'ensemble du secteur financier au sein de l'Union européenne.

- Constatant une tendance récurrente à l'alourdissement des sanctions dans le secteur financier, la Chambre de Commerce s'interroge quant à la proportionnalité d'une amende administrative d'un montant maximal pouvant aller jusqu'à 5.000.000 euros, telle que prévue par le Projet.

- Elle souhaite aussi souligner que toute mesure technologique trop prescriptive pourrait devenir rapidement obsolète en raison d'une évolution technologique très rapide. En effet, si une approche coordonnée de la cyber-résilience est importante, il est également important de préserver la flexibilité de l'innovation.

- La Chambre de Commerce est en mesure d'approuver le Projet, sous réserve de la prise en compte de ses remarques.

Considérations générales

Force est de constater qu'au cours des dernières décennies, l'utilisation des technologies de l'information et de la communication (ci-après les « TIC ») est devenue centrale dans la fourniture de services financiers, au point qu'elles ont désormais acquis une importance cruciale dans l'exécution des fonctions quotidiennes typiques de toutes les entités financières.

Cependant, le degré croissant de numérisation et d'interconnexion accentue également le risque lié aux TIC, ce qui expose davantage la société dans son ensemble, et le système financier en particulier, aux cybermenaces ou aux dysfonctionnements des TIC. Si l'utilisation généralisée de systèmes de TIC ainsi qu'une numérisation et une connectivité poussées sont aujourd'hui des caractéristiques essentielles des activités des entités financières de l'Union européenne, le cadre législatif relatif à la résilience opérationnelle numérique et à la sécurité des TIC n'est pas encore totalement ou systématiquement harmonisé, alors que la résilience opérationnelle numérique est indispensable pour garantir la stabilité financière et l'intégrité du marché à l'ère numérique[2].

Le législateur européen a ainsi estimé qu'un corpus réglementaire unique et un système de surveillance devraient être développés pour couvrir la résilience opérationnelle numérique ; les mandats des autorités compétentes devraient ainsi être renforcés pour leur permettre de superviser la gestion du risque lié aux TIC dans le secteur financier afin de protéger l'intégrité et l'efficacité du marché intérieur et de faciliter son bon fonctionnement. Par conséquent, le **Règlement 2022/2554** vient harmoniser et renforcer les exigences en matière des TIC afin d'atteindre un niveau élevé de résilience opérationnelle numérique pour l'ensemble du secteur financier au sein de l'Union européenne.

Comme indiqué dans l'exposé des motifs, cette consolidation et l'harmonisation des exigences clés en matière de résilience opérationnelle numérique s'inscrivent dans l'objectif de favoriser l'innovation et l'adoption de nouvelles technologies dans le secteur financier, tout en assurant la stabilité financière et la protection des investisseurs et des consommateurs.

Le Règlement 2022/2554 établit un corpus de règles uniformes sur la résilience opérationnelle numérique en vertu duquel les entités visées devront s'assurer qu'elles peuvent résister, répondre et se rétablir face à toute perturbation opérationnelle grave liée aux TIC. Il définit notamment des exigences uniformes en ce qui concerne la gestion des risques liés aux TIC, la notification des incidents majeurs liés aux TIC, les tests de résilience opérationnelle numérique, le partage d'informations en rapport avec les cybermenaces et les mesures destinées à garantir la gestion saine du risque lié aux prestataires tiers de services TIC. Les dispositions du Règlement 2022/2554 prévoient aussi des règles relatives à l'établissement du cadre de supervision applicable aux prestataires tiers critiques de services TIC.

Etant donné que les dispositions du Règlement 2022/2554 sont directement applicables dans les Etats membres, dont le Luxembourg, le Projet se limite à (i) désigner les autorités compétentes au Luxembourg chargées de veiller à l'application du Règlement 2022/2554 par les personnes soumises à leur surveillance (à savoir, la Commission de surveillance du secteur financier et le Commissariat aux assurances), (ii) à doter lesdites autorités compétentes de pouvoir de surveillance et d'enquête nécessaires à l'exercice de leurs fonctions ainsi qu'à (iii) établir un régime de sanctions et d'autres mesures administratives. Dans ce contexte, la Chambre de Commerce observe et ce depuis quelques années une tendance récurrente à l'alourdissement des sanctions, tant administratives que pénales, notamment dans le secteur financier. Elle s'interroge à cet égard quant à la proportionnalité d'une amende administrative d'un montant maximal pouvant aller jusqu'à 5.000.000 euros, telle que prévue par le Projet tant pour les personnes morales que pour les personnes physiques.

Quant à la **Directive 2022/2556**, cette dernière vient modifier les directives européennes sectorielles[3] afin d'assurer leur cohérence avec les dispositions du Règlement 2022/2554. En effet,

[2] Considérants du Règlement 2022/2554

[3] Directive 2009/65/CE du Parlement européen et du Conseil du 13 juillet 2009 portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières ;

lesdites directives sectorielles prévoient à l'heure actuelle les exigences liées à la gestion du risque lié aux TIC auquel est exposé le secteur financier de manière diverse et incomplète et certaines ne les prévoient tout simplement pas.

Par conséquent, le Projet opère, outre la mise en œuvre du Règlement 2022/2554, la transposition en droit luxembourgeois de ces modifications ponctuelles apportées auxdites directives européennes et ayant trait à la résilience numérique et à la sécurité des TIC.

La Chambre de Commerce n'a pas de commentaires quant aux dispositions du Projet. Elle souhaite néanmoins souligner que toute mesure technologique trop prescriptive pourrait devenir rapidement obsolète en raison d'une évolution technologique très rapide. En effet, si une approche coordonnée de la cyber-résilience est importante, il est également important de préserver la flexibilité de l'innovation, car « *une taille unique ne convient pas à tout le monde* ».

* * *

Après consultation de ses ressortissants, la Chambre de Commerce peut approuver le projet de loi sous avis, sous réserve de la prise en compte de ses remarques.

GKA/DJI

Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II) ;

Directive 2011/61/UE du Parlement européen et du Conseil du 8 juin 2011 sur les gestionnaires de fonds d'investissement alternatifs et modifiant les directives 2003/41/CE et 2009/65/CE ainsi que les règlements (CE) n° 1060/2009 et (UE) n° 1095/2010 ;

Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE ;

Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement et modifiant la directive 82/891/CEE du Conseil ainsi que les directives du Parlement européen et du Conseil 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE et 2013/36/UE et les règlements du Parlement européen et du Conseil (UE) n° 1093/2010 et (UE) n° 648/2012 ;

Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE ;

Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE ;

Directive (UE) 2016/2341 du Parlement européen et du Conseil du 14 décembre 2016 concernant les activités et la surveillance des institutions de retraite professionnelle (IRP).