COMMISSION
EUROPÉENNE

Bruxelles, le 24.9.2020
COM(2020) 596 final

2020/0268 (COD)

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

(Texte présentant de l'intérêt pour l'EEE)

{SEC(2020) 309 final} - {SWD(2020) 203 final} - {SWD(2020) 204 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Motivation et objectifs de la proposition

La présente proposition fait partie d'un train de mesures destinées à libérer et à renforcer tout le potentiel que la finance numérique peut offrir sur les plans de l'innovation et de la concurrence, tout en en maîtrisant les risques qui en découlent. Elle est conforme aux priorités de la Commission consistant à adapter l'Europe à l'ère du numérique et bâtir une économie au service des personnes et parée pour l'avenir. L'ensemble de mesures sur la finance numérique comprend une nouvelle stratégie en matière de finance numérique pour le secteur financier de l'Union[1]. Celle-ci a pour objectif de garantir que l'Union européenne s'engage dans la révolution numérique et en soit le moteur, avec en tête des entreprises européennes innovantes, en faisant profiter les entreprises et les consommateurs européens des avantages de la finance numérique. Outre cette proposition, le train de mesures comprend également une proposition de règlement sur les marchés de crypto-actifs[2], une proposition de règlement sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués (DLT)[3] et une proposition de règlement sur la résilience opérationnelle numérique du secteur financier[4].

La motivation et les objectifs qui sous-tendent les deux ensembles de mesures législatives ont été précisés dans les exposés des motifs, respectivement, de la proposition de règlement sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, de la proposition de règlement sur les marchés de crypto-actifs et de la proposition de règlement sur la résilience opérationnelle numérique et s'appliquent également ici. La motivation particulière de la présente proposition de directive tient au fait que, pour garantir la sécurité juridique en ce qui concerne les crypto-actifs et atteindre les objectifs de renforcement de la résilience opérationnelle numérique, il convient de prévoir une exemption temporaire pour les systèmes multilatéraux de négociation et de modifier ou de clarifier certaines dispositions des directives européennes en vigueur sur les services financiers.

• Cohérence avec les dispositions existantes dans le domaine d'action

Cette proposition, à l'instar des propositions de règlement qu'elle accompagne, s'inscrit dans le cadre d'un travail plus vaste actuellement mené aux échelles européenne et internationale dans le but i) de renforcer la cybersécurité dans les services financiers et d'aborder les risques opérationnels plus larges, et ii) de fournir un cadre juridique européen clair, proportionné et facilitant pour les prestataires de services sur crypto-actifs.

---

1 Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, à la Banque centrale européenne, au Comité économique et social européen et au Comité des régions sur une stratégie en matière de finance numérique pour l'UE, 23 septembre 2020, COM(2020) 591.

2 Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937, COM(2020) 593.

3 Proposition de règlement du Parlement européen et du Conseil sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, COM(2020) 594.

4 Proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014, COM(2020) 595.

- **Cohérence avec les autres politiques de l'Union**

Comme l'a déclaré la présidente von der Leyen dans ses orientations politiques[5], et comme le précise la communication intitulée «Façonner l'avenir numérique de l'Europe»[6], il est essentiel que l'Europe tire profit de tous les avantages offerts par l'ère numérique et renforce sa capacité industrielle et d'innovation, au sein d'un cadre garant de la sécurité et de l'éthique.

S'agissant des crypto-actifs, cette proposition est étroitement liée aux politiques plus générales de la Commission sur la technologie de la chaîne de blocs, étant donné que les crypto-actifs, en tant que principale application des technologies de la chaîne de blocs, sont inextricablement liés à la promotion de ces technologies à travers l'Europe.

Pour ce qui est de la résilience opérationnelle, la stratégie européenne pour les données[7] définit quatre piliers – la protection des données, les droits fondamentaux, la sûreté et la cybersécurité – comme des conditions préalables essentielles pour une société à laquelle les données confèrent les moyens dont elle a besoin. Un cadre législatif destiné à renforcer la résilience opérationnelle numérique des entités financières de l'Union est conforme à ces objectifs politiques. La proposition viendrait également appuyer les stratégies en faveur de la reprise à la suite du coronavirus, car elle garantirait que la dépendance accrue à l'égard de la finance numérique va de pair avec la résilience opérationnelle. Les deux propositions répondent également aux appels du forum de haut niveau sur l'UMC visant à établir des règles claires pour l'utilisation des crypto-actifs (recommandation 7) et à mettre en place de nouvelles règles sur la cyberrésilience (recommandation 10)[8].

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La présente proposition de directive est fondée sur l'article 53, paragraphe 1, et l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE).

- **Subsidiarité (en cas de compétence non exclusive)**

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

- **Proportionnalité**

---

5 Présidente Ursula von der Leyen, *Orientations politiques pour la prochaine Commission européenne, 2019-2024*, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_fr.pdf.

6 Communication de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Façonner l'avenir numérique de l'Europe*, COM(2020) 67 final.

7

8 Forum de haut niveau sur l'union des marchés des capitaux, «A new vision for Europe's capital markets: final report», 2020,https://ec.europa.eu/info/sites/info/files/business_economy_euro/growth_and_investment/documents/200610-cmu-high-level-forum-final-report_en.pdf.

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

- **Choix de l'instrument**

La présente proposition de directive accompagne les propositions de règlements sur les marchés de crypto-actifs; sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique. Ces règlements énoncent i) les principales règles applicables aux prestataires de services sur crypto-actifs, ii) les conditions qui régissent le régime pilote pour les infrastructures de marché DLT; et iii) les principales règles qui régissent la gestion des risques informatiques, la notification des incidents, les tests et la supervision. Pour atteindre les objectifs fixés dans ces règlements, il est également nécessaire de prévoir une exemption temporaire pour les systèmes multilatéraux de négociation et de modifier plusieurs directives du Parlement européen et du Conseil adoptées sur la base de l'article 53, paragraphe 1, et de l'article 114 du TFUE. La présente proposition de directive est par conséquent nécessaire pour modifier ces directives.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Évaluations ex post/bilans de qualité de la législation existante**

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

- **Consultation des parties intéressées**

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

- **Obtention et utilisation d'expertise**

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

- **Analyse d'impact**

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

- **Réglementation affûtée et simplification**

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

- **Droits fondamentaux**

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

4. INCIDENCE BUDGÉTAIRE

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

Voir les exposés des motifs des propositions de règlements sur les marchés de crypto-actifs, sur un régime temporaire pour les infrastructures de marché DLT et sur la résilience opérationnelle numérique.

- **Explication détaillée de certaines dispositions de la proposition**

Tous les articles sont liés à la proposition de règlement sur la résilience opérationnelle numérique et la complètent. Ils modifient les différentes exigences en matière de risque opérationnel ou de gestion des risques prévues dans 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 du Parlement européen et du Conseil, en introduisant des références croisées précises dans ces dispositions et en assurant ainsi la clarté juridique. Plus précisément:

– les articles 2 à 4, 6 et 8 modifient la directive 2009/65/CE portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières (OPCVM)[9], la directive 2009/138/CE sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II)[10], la directive 2011/61/UE sur les gestionnaires de fonds d'investissement alternatifs[11], la directive 2014/56/UE concernant les contrôles légaux des comptes annuels et des comptes consolidés[12] et la directive (UE) 2016/2341 concernant les activités et la surveillance des institutions de retraite professionnelle (IRP)[13], et ont pour but d'introduire dans chacune de ces directives des références croisées spécifiques au règlement (UE) 2021/xx [DORA] concernant la gestion des systèmes et outils informatiques de ces entités financières qui devrait se faire conformément aux dispositions dudit règlement.

9 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 (JO L 302 du 17.11.2009, p. 32).

10 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 (JO L 335 du 17.12.2009, p. 1).

11 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) nº 1060/2009 et (UE) nº 1095/2010 (JO L 174 du 1.7.2011, p. 1).

12 Directive 2014/56/UE du Parlement européen et du Conseil du 16 avril 2014 modifiant la directive 2006/43/CE concernant les contrôles légaux des comptes annuels et des comptes consolidés (JO L 158 du 27.5.2014, p. 196).

13 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 (JO L 354 du 23.12.2016, p. 37).

– L'article 5 modifie les exigences de la directive 2013/36/UE (directive sur les exigences de fonds propres, CRD)[14] relatives aux plans d'urgence et de poursuite de l'activité afin d'y inclure les plans de continuité des activités informatiques et de rétablissement après sinistre dans le domaine informatique établis conformément aux dispositions du règlement (UE) 2021/xx [DORA].

– L'article 6 modifie la directive 2014/65/UE concernant les marchés d'instruments financiers (MIFID2) en y ajoutant des références croisées au règlement (UE) 2021/xx [DORA] et en modifiant les dispositions relatives à la continuité et à la régularité de la fourniture de services d'investissement et de l'exercice d'activités d'investissement, à la résilience et à la capacité suffisante des systèmes de négociation, aux mécanismes efficaces de continuité des activités et à la gestion des risques.

– L'article 7 modifie la directive (UE) 2015/2366 concernant les services de paiement dans le marché intérieur (DSP2)[15] et plus précisément les règles d'agrément en introduisant une référence croisée au règlement (UE) 2021/xx [DORA]. En outre, les règles relatives à la notification des incidents contenues dans ladite directive devraient exclure la notification des incidents informatiques que le règlement (UE) 2021/xx [DORA] harmonise pleinement.

Le premier paragraphe de l'article 6 contribue en outre à clarifier le traitement juridique des crypto-actifs qui peuvent être qualifiés d'instruments financiers. Pour ce faire, il modifie la définition d'un «instrument financier» au sens de la directive 2014/65/UE concernant les marchés d'instruments financiers afin de préciser, au-delà de tout doute juridique, que ces instruments peuvent être émis sur la base d'une technologie des registres distribués.

Le quatrième paragraphe de l'article 6 complète la proposition de règlement sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués en exemptant temporairement ces infrastructures de certaines dispositions de la directive 2014/65/UE afin de leur permettre de mettre au point des solutions pour la négociation et le règlement des transactions sur les crypto-actifs qui seraient qualifiés d'instruments financiers.

[14] 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 et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

[15] 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) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35)

2020/0268 (COD)

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

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 53, paragraphe 1, et son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis de la Banque centrale européenne[16],

vu l'avis du Comité économique et social européen[17],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) L'Union doit traiter de manière adéquate et globale les risques numériques auxquels sont exposées toutes les entités financières et qui découlent d'un recours accru aux technologies de l'information et de la communication (TIC) dans la fourniture et la consommation de services financiers.

(2) Les opérateurs du secteur financier sont fortement tributaires de l'utilisation des technologies numériques dans leurs activités quotidiennes; il est donc primordial de garantir la résilience opérationnelle de leurs opérations numériques face aux risques informatiques. Ce besoin est devenu encore plus pressant en raison de la croissance du marché des technologies de pointe, qui permettent notamment de transférer et de stocker par voie électronique des représentations numériques de valeur ou de droits, en utilisant la technologie des registres distribués ou une technologie similaire («crypto-actifs»), et des services liés à ces actifs.

(3) Au niveau de l'Union, les exigences liées au risque informatique dans le secteur financier sont actuellement réparties entre les directives 2006/43/CE[18],

[16] JO C … du …, p. ….

[17] JO C du, p. .

[18] Directive 2006/43/CE du Parlement européen et du Conseil du 17 mai 2006 concernant les contrôles légaux des comptes annuels et des comptes consolidés et modifiant les directives 78/660/CEE et 83/349/CEE du Conseil, et abrogeant la directive 84/253/CEE du Conseil (JO L 157 du 9.6.2006, p. 87).

2009/66/CE[19], 2009/138/CE[20], 2011/61/CE[21], 2013/36/UE[22], 2014/65/UE[23], (UE) 2015/2366[24] et (UE) 2016/2341[25] du Parlement européen et du Conseil, et sont diverses et parfois incomplètes. Dans certains cas, le risque informatique n'a été abordé qu'implicitement dans le cadre du risque opérationnel, alors que dans d'autres, il n'a tout simplement pas été pris en considération. Il convient de remédier à cette situation en procédant à l'alignement du règlement (UE) xx/20xx du Parlement européen et du Conseil [DORA][26] et de ces actes. La présente directive propose une série de modifications qui semblent nécessaires pour apporter une clarté et une cohérence juridiques en ce qui concerne l'application, par les entités financières agréées et soumises à une surveillance conformément auxdites directives, de diverses exigences en matière de résilience opérationnelle numérique qui sont nécessaires à l'exercice de leurs activités, et garantir ainsi le bon fonctionnement du marché intérieur.

(4) Dans le domaine des services bancaires, la directive 2013/36/UE concernant l'accès à l'activité des établissements de crédit et la réglementation prudentielle des établissements de crédit et des entreprises d'investissement n'énonce actuellement que des règles générales de gouvernance interne et des dispositions relatives au risque opérationnel définissant des exigences en matière de plans d'urgence et de poursuite de l'activité qui servent implicitement de base pour aborder la gestion des risques informatiques. Toutefois, pour veiller à ce que le risque informatique soit explicitement pris en considération, les exigences relatives aux plans d'urgence et de poursuite de l'activité devraient être modifiées de manière à inclure les plans de continuité des activités et de rétablissement après sinistre ayant trait également aux risques informatiques, conformément aux exigences définies dans le règlement (UE) 2021/xx [DORA].

(5) La directive 2014/65/UE concernant les marchés d'instruments financiers fixe des règles plus strictes en matière de TIC pour les entreprises d'investissement et les

---

19 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 (OPCVM) (JO L 302 du 17.11.2009, p. 32).

20 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) (JO L 335 du 17.12.2009, p. 1).

21 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) nº 1060/2009 et (UE) nº 1095/2010 (JO L 174 du 1.7.2011, p. 1).

22 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 et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

23 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 (JO L 173 du 12.6.2014, p. 349).

24 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) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

25 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) (JO L 354 du 23.12.2016, p. 37).

26 JO L […] du […], p. […].

plateformes de négociation uniquement lorsqu'elles se livrent au trading algorithmique. Des exigences moins détaillées s'appliquent aux services de communication de données et aux référentiels centraux. En outre, elle ne comporte que des références limitées aux dispositifs de contrôle et de sauvegarde des systèmes de traitement de l'information et à l'utilisation de systèmes, de ressources et de procédures appropriés pour garantir la continuité et la régularité des services opérationnels. Cette directive devrait être alignée sur le règlement (UE) 2021/xx [DORA] en ce qui concerne la continuité et la régularité de la fourniture de services d'investissement et de l'exercice d'activités d'investissement, la résilience opérationnelle, la capacité des systèmes de négociation, et l'efficacité des mécanismes de continuité des activités et de la gestion des risques.

(6) Actuellement, la définition d'un «instrument financier» au sens de la directive 2014/65/UE n'inclut pas explicitement les instruments financiers émis au moyen d'une catégorie de technologies qui permettent l'enregistrement distribué de données cryptées (technologie des registres distribués, ou «DLT»). Afin de garantir que ces instruments financiers puissent être négociés sur le marché en vertu du cadre juridique actuel, la définition de la directive 2014/65/UE devrait être modifiée de façon à les y inclure.

(7) En particulier, afin de permettre le développement de crypto-actifs qui seraient qualifiés d'instruments financiers et de la DLT, tout en préservant un niveau élevé de stabilité financière, d'intégrité du marché, de transparence et de protection des investisseurs, il serait utile de créer un régime temporaire pour les infrastructures de marché DLT. Ce cadre juridique temporaire devrait permettre aux autorités compétentes d'autoriser temporairement les infrastructures de marché DLT à opérer selon un ensemble d'exigences en matière d'accès à celles-ci différentes de celles qui sont par ailleurs applicables en vertu de la législation de l'Union sur les services financiers et qui sont susceptibles de les empêcher de mettre au point des solutions pour la négociation et le règlement des transactions sur crypto-actifs qui peuvent être qualifiés d'instruments financiers. Ce cadre juridique devrait être temporaire afin de permettre aux autorités européennes de surveillance (AES) et aux autorités nationales compétentes d'acquérir de l'expérience quant aux perspectives et aux risques spécifiques que présentent les crypto-actifs négociés sur ces infrastructures. La présente directive accompagne donc le règlement [sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués] en étayant ce nouveau cadre réglementaire de l'Union sur les infrastructures de marché DLT au moyen d'une exemption ciblée de certaines dispositions de la législation de l'Union sur les services financiers applicables aux activités et services liés aux instruments financiers définis à l'article 4, paragraphe 1, point 15), de la directive 2014/65/UE qui, autrement, n'offriraient pas toute la souplesse requise pour le déploiement de solutions dans les phases de négociation et de post-négociation des transactions portant sur des crypto-actifs.

(8) Un système multilatéral de négociation DLT devrait consister en un système multilatéral, exploité par une entreprise d'investissement ou un opérateur de marché agréé en vertu de la directive 2014/65/UE, qui a reçu une autorisation spécifique en vertu du règlement (UE) xx/20xx du Parlement européen et du Conseil[27] [Proposition de règlement sur un régime pilote pour les infrastructures de marché DLT]. Les

[27] [titre complet] (JO L […] du […], p. […]).

systèmes multilatéraux de négociation DLT devraient être soumis à toutes les exigences applicables à un système multilatéral de négociation en vertu de ladite directive, sauf si l'autorité nationale compétente leur accorde une exemption en vertu de la présente directive. Un éventuel obstacle réglementaire au développement d'un système multilatéral de négociation de valeurs mobilières émises sur une DLT pourrait venir de l'obligation d'intermédiation énoncée dans la directive 2014/65/UE. Un système multilatéral de négociation traditionnel ne peut admettre comme membres et participants que des entreprises d'investissement, des établissements de crédit et d'autres personnes qui possèdent un niveau suffisant d'aptitude et de compétence pour la négociation et qui disposent d'une organisation et de ressources connexes appropriées. Un système multilatéral de négociation DLT devrait être autorisé à demander une dérogation à cette obligation afin de permettre aux investisseurs de détail d'accéder facilement à la plateforme de négociation, à condition que des garanties adéquates soient mises en place en matière de protection des investisseurs.

(9) La directive (UE) 2015/2366 concernant les services de paiement 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. Ces règles d'agrément devraient être modifiées afin d'être alignées sur le règlement (UE) 2021/xx [DORA]. En outre, les règles relatives à la notification des incidents contenues dans ladite directive ne devraient pas s'appliquer aux notifications des incidents informatiques, que le règlement (UE) 2021/xx [DORA] harmonise pleinement.

(10) Les directives 2009/138/CE sur l'accès à l'activité de l'assurance et de la réassurance et leur exercice et (UE) 2016/2341 concernant les activités et la surveillance des institutions de retraite professionnelle intègrent en partie le risque informatique dans leurs dispositions générales sur la gouvernance et la gestion des risques, tandis que certaines exigences doivent être précisées par des règlements délégués avec ou sans référence spécifique au risque informatique. Des dispositions encore moins spécifiques s'appliquent aux contrôleurs légaux des comptes et aux cabinets d'audit, puisque la directive 2014/56/UE du Parlement européen et du Conseil[28] ne contient que des dispositions d'ordre général sur l'organisation interne. De même, seules des règles très générales s'appliquent aux gestionnaires de fonds d'investissement alternatifs et aux sociétés de gestion relevant des directives 2011/61/UE et 2009/65/CE. Ces directives devraient dès lors être alignées sur les exigences définies dans le règlement (UE) 2021/xx [DORA] en ce qui concerne la gestion des systèmes et outils informatiques.

(11) Dans de nombreux cas, des exigences supplémentaires en matière de TIC ont déjà été établies dans des actes délégués et d'exécution, qui ont été adoptés sur la base de projets de normes techniques de réglementation et d'exécution élaborés par l'AES compétente. Afin de garantir la clarté juridique sur le fait que la base juridique régissant les dispositions relatives aux risques informatiques découle désormais exclusivement du règlement (UE) 2021/xx [DORA], les habilitations prévues par ces directives devraient être modifiées afin de préciser que les dispositions relatives aux risques informatiques ne relèvent pas desdites habilitations.

[28] Directive 2014/56/UE du Parlement européen et du Conseil du 16 avril 2014 modifiant la directive 2006/43/CE concernant les contrôles légaux des comptes annuels et des comptes consolidés (JO L 158 du 27.5.2014, p. 196).

(12) Pour assurer une application cohérente et simultanée du règlement (UE) xx/20xx [DORA] et de la présente directive, qui constituent ensemble le nouveau cadre en matière de résilience opérationnelle numérique du secteur financier, les États membres devraient appliquer les dispositions de droit national transposant la présente directive à partir de la date d'application dudit règlement.

(13) Les directives 2006/43/CE, 2009/66/CE, 2009/138/CE, 2011/61/CE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 ont été adoptées sur les bases de l'article 53, paragraphe 1, et de l'article 114 du traité sur le fonctionnement de l'Union européenne. Les modifications contenues dans la présente directive devraient être incluses dans un acte unique en raison de l'interdépendance du sujet et des objectifs des modifications, et cet acte unique devrait être adopté sur la base à la fois de l'article 53, paragraphe 1, et de l'article 114 du traité sur le fonctionnement de l'Union européenne.

(14) Étant donné que les objectifs de la présente directive ne peuvent pas être réalisés de manière suffisante par les États membres, puisqu'ils supposent l'harmonisation par la mise à jour et la modification d'exigences déjà contenues dans des directives, mais peuvent, en raison des dimensions et des effets de l'action envisagée, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(15) Conformément à la déclaration politique commune des États membres et de la Commission du 28 septembre 2011 sur les documents explicatifs[29], les États membres se sont engagés à joindre à la notification de leurs mesures de transposition, dans les cas où cela se justifie, un ou plusieurs documents expliquant le lien entre les éléments d'une directive et les parties correspondantes des instruments nationaux de transposition. En ce qui concerne la présente directive, le législateur estime que la transmission de ces documents est justifiée,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Modifications de la directive 2006/43/CE

À l'article 24 *bis*, paragraphe 1, de la directive 2006/43/CE, le point b) est remplacé par le texte suivant:

«b) le contrôleur légal des comptes ou le cabinet d'audit dispose de procédures administratives et comptables saines, de mécanismes internes de contrôle qualité, de procédures efficaces d'évaluation des risques et de dispositifs efficaces de contrôle et de protection afin de gérer ses systèmes et outils informatiques conformément à l'article 6 du règlement (UE) 2021/xx [DORA] du Parlement européen et du Conseil*.

_____

[29] JO C 369 du 17.12.2011, p. 14.

* [*titre complet*] (JO L […] du […], p. […]).»

Article 2

Modifications de la directive 2009/65/CE

L'article 12 de la directive 2009/65/CE est modifié comme suit:

(1) au paragraphe 1, point a), le deuxième alinéa est remplacé par le texte suivant:

«a) ait une bonne organisation administrative et comptable, des dispositifs de contrôle et de sécurité dans le domaine informatique, y compris des systèmes de technologies de l'information et de la communication qui sont mis en place et gérés conformément à l'article 6 du règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA], ainsi que des mécanismes de contrôle interne adéquats incluant, notamment, des règles concernant les opérations personnelles de ses salariés ou la détention ou la gestion de placements dans des instruments financiers en vue d'investir pour son propre compte, et garantissant, au minimum, que chaque transaction concernant l'OPCVM peut être reconstituée quant à son origine, aux parties concernées, à sa nature, ainsi qu'au moment et au lieu où elle a été effectuée, et que les actifs des OPCVM gérés par la société de gestion sont placés conformément au règlement du fonds ou aux documents constitutifs et aux dispositions légales en vigueur;

---

* [*titre complet*] (JO L […] du […], p. […]).»

(2) Le paragraphe 3 est remplacé par le texte suivant:

«3. Sans préjudice de l'article 116, la Commission adopte, par voie d'actes délégués en conformité avec l'article 112 *bis*, des mesures précisant:

a) les procédures et les dispositifs visés au paragraphe 1, deuxième alinéa, point a), autres que ceux ayant trait à la gestion des risques liés aux technologies de l'information et de la communication;

b) les structures et les conditions d'organisation destinées à restreindre au minimum les conflits d'intérêts, visées au paragraphe 1, deuxième alinéa, point b). »

Article 3

Modifications de la directive 2009/138/CE

La directive 2009/138/CE est modifiée comme suit:

(1) À l'article 41, le paragraphe 4 est remplacé par le texte suivant:

«4. Les entreprises d'assurance et de réassurance prennent des mesures raisonnables afin de veiller à la continuité et à la régularité dans l'accomplissement de leurs activités, y compris par l'élaboration de plans d'urgence. À cette fin, elles utilisent des systèmes, des ressources et des procédures appropriés et proportionnés, mettent en place des systèmes de technologies de l'information et de la communication et

gèrent ceux-ci conformément à l'article 6 du règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA].»

---

* [*titre complet*] (JO L […] du […], p. […]).

(2) À l'article 50, paragraphe 1, les points a) et b) sont remplacés par le texte suivant:

«a) les éléments des systèmes visés aux articles 41, 44, 46 et 47, autres que les éléments concernant la gestion des risques liés aux technologies de l'information et de la communication, et les domaines visés à l'article 44, paragraphe 2;»;

b) les fonctions respectivement prévues aux articles 44, 46, 47 et 48, autres que les fonctions relatives à la gestion des risques liés aux technologies de l'information et de la communication.»

Article 4

Modifications de la directive 2011/61/CE

L'article 18 de la directive 2011/61/CE est remplacé par le texte suivant:

«*Article 18*

Principes généraux

1. Les États membres exigent des gestionnaires qu'ils utilisent à tout moment les ressources humaines et techniques adaptées et appropriées nécessaires pour la bonne gestion des FIA.

En particulier, les autorités compétentes de l'État membre d'origine du gestionnaire, compte tenu aussi de la nature des FIA gérés par le gestionnaire, exigent que celui-ci ait de solides procédures administratives et comptables, des dispositifs de contrôle et de sauvegarde pour la gestion des systèmes de technologie de l'information et de la communication requis par l'article 6 du [règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA]], ainsi que des mécanismes de contrôle interne adéquats incluant, notamment, des règles concernant les transactions personnelles de ses employés ou la participation ou la gestion d'investissements en vue d'investir pour son propre compte et garantissant, au minimum, que chaque transaction concernant les FIA peut être reconstituée quant à son origine, aux parties concernées, à sa nature, ainsi qu'au moment et au lieu où elle a été effectuée, et que les actifs des FIA gérés par le gestionnaire sont placés conformément au règlement du FIA ou à ses documents constitutifs et aux dispositions légales en vigueur.

2. La Commission adopte par voie d'actes délégués, en conformité avec l'article 56 et dans le respect des conditions fixées par les articles 57 et 58, des mesures précisant les procédures et les dispositifs visés au paragraphe 1, autres que pour les systèmes de technologies de l'information et de la communication.

---

* [*titre complet*] (JO L […] du […], p. […]).»

Article 5

Modification de la directive 2013/36/UE

À l'article 85 de la directive 2013/36/UE, le paragraphe 2 est remplacé par le texte suivant:

«2. Les autorités compétentes veillent à ce que les établissements disposent de plans d'urgence et de poursuite de l'activité adéquats, y compris des plans de continuité des activités et de reprise après sinistre pour la technologie qu'ils utilisent pour la communication d'informations ("technologie de l'information et de la communication") établis conformément à l'article 6 du règlement (UE) 2021/xx du Parlement européen et du Conseil [DORA]*, afin qu'ils puissent poursuivre leurs activités en cas de grave perturbation de celles-ci et limiter les pertes subies à la suite d'une telle perturbation.

---

* [*titre complet*] (JO L […] du […], p. […]).»

Article 6

Modifications de la directive 2014/65/UE

La directive 2014/65/UE est modifiée comme suit:

(1) À l'article 4, paragraphe 1, le point 15) est remplacé par le texte suivant:

«"instruments financiers", les instruments visés à la section C de l'annexe I, y compris lorsqu'ils sont émis au moyen de la technologie des registres distribués;»

(2) L'article 16 est modifié comme suit:

(a) Le paragraphe 4 est remplacé par le texte suivant:

«4. Toute entreprise d'investissement prend des mesures raisonnables pour garantir la continuité et la régularité de la fourniture de ses services d'investissement et de l'exercice de ses activités d'investissement. À cette fin, elle utilise des systèmes appropriés et proportionnés, y compris des systèmes de technologies de l'information et de la communication ("TIC") mis en place et gérés conformément à l'article 6 du règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA], ainsi que des ressources et des procédures appropriées et proportionnées.»

(b) Au paragraphe 5, les deuxième et troisième alinéas sont remplacés par le texte suivant:

«Toute entreprise d'investissement dispose de procédures comptables et administratives saines, de mécanismes de contrôle interne et de techniques efficaces d'évaluation des risques.

Sans préjudice de la capacité des autorités compétentes d'exiger l'accès aux communications conformément à la présente directive et au règlement (UE) nº 600/2014, toute entreprise d'investissement dispose de mécanismes de sécurité solides pour garantir, conformément aux exigences du règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA], la sécurité et l'authentification des moyens de transfert de l'information, réduire au minimum le risque de corruption des données et d'accès non autorisé et empêcher les fuites d'informations afin de maintenir en permanence la confidentialité des données.»

(3) L’article 17 est modifié comme suit:

(a) Le paragraphe 1 est remplacé par le texte suivant:

«1. Une entreprise d’investissement recourant au trading algorithmique dispose de systèmes et contrôles des risques efficaces et adaptés à son activité pour garantir que ses systèmes de négociation sont résilients et ont une capacité suffisante au regard des exigences énoncées au chapitre II du règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA], qu’ils sont soumis à des seuils et limites de négociation appropriés et qu’ils préviennent l’envoi d’ordres erronés ou tout autre fonctionnement des systèmes susceptible de donner naissance ou de contribuer à une perturbation du marché.

Elle dispose également de systèmes et contrôles des risques efficaces pour garantir que ses systèmes de négociation ne peuvent être utilisés à aucune fin contraire au règlement (UE) nº 596/2014 ou aux règles d’une plate-forme de négociation à laquelle elle est connectée.

Elle dispose enfin de plans de continuité des activités efficaces pour faire face à toute défaillance de ses systèmes de négociation, y compris des plans de continuité des activités et de reprise après sinistre concernant la technologie de l’information et de la communication établis conformément à l’article 6 du règlement (UE) 2021/xx du Parlement européen et du Conseil [DORA], et elle veille à ce que ses systèmes soient entièrement testés et convenablement suivis de manière à garantir qu’ils satisfont aux exigences générales du présent paragraphe et aux exigences spécifiques prévues aux chapitres II et IV du règlement (UE) 2021/xx [DORA].»

(b) Au paragraphe 7, le point a) est remplacé par le texte suivant:

«a) le détail des exigences organisationnelles prévues aux paragraphes 1 à 6, autres que celles liées à la gestion des risques informatiques, qu’il convient d’imposer aux entreprises d’investissement fournissant différents services d’investissement, différentes activités d’investissement, des services auxiliaires ou offrant une combinaison de ces services, selon lequel les précisions relatives aux exigences organisationnelles visées au paragraphe 5 comportent, pour l’accès direct au marché et l’accès sponsorisé, des exigences particulières propres à permettre que les contrôles appliqués à l’accès sponsorisé soient au minimum équivalents à ceux appliqués à l’accès direct au marché;»

(4) À l’article 19, le paragraphe suivant est ajouté:

«3. Toutefois, lorsque l’entreprise d’investissement ou l’opérateur de marché exploite un système multilatéral de négociation reposant sur la technologie des registres distribués (“système multilatéral de négociation DLT”) tel que défini à l’article 2, paragraphe 3, du règlement (UE) xx/20xx [proposition de règlement sur un régime pilote pour les infrastructures de marché DLT], l’autorité compétente peut autoriser, en vertu de ses règles régissant l’accès visées à l’article 18, paragraphe 3, et pour une durée maximale de quatre ans, l’entreprise d’investissement ou l’opérateur de marché à admettre des personnes physiques au système multilatéral de négociation DLT en tant que membres ou participants, à condition que ces personnes remplissent les conditions suivantes:

(a) elles jouissent d’une honorabilité suffisante et répondent à tous les impératifs de compétence; et

(b) elles présentent un niveau suffisant d'aptitude, de compétence et d'expérience, y compris une connaissance de la négociation et du fonctionnement de la technologie des registres distribués ("DLT").

Lorsqu'une autorité compétente accorde l'exemption visée au premier alinéa, elle peut imposer des mesures supplémentaires de protection des investisseurs pour la protection des personnes physiques admises comme membres ou participants au système multilatéral de négociation DLT. Ces mesures sont proportionnées au profil de risque des participants ou membres»

(5) À l'article 47, le paragraphe 1 est modifié comme suit:

(a) Le point b) est remplacé par le texte suivant:

«b) qu'ils soient adéquatement équipés pour gérer les risques auxquels ils sont exposés, y compris les risques liés aux systèmes et outils informatiques conformément à l'article 6 du règlement (UE) 2021/xx [DORA]*, qu'ils mettent en œuvre des dispositifs et des systèmes appropriés leur permettant d'identifier tous les risques significatifs pouvant compromettre leur bon fonctionnement, et qu'ils instaurent des mesures effectives pour atténuer ces risques.»

(b) Le point c) est supprimé;

(6) L'article 48 est modifié comme suit:

(a) Le paragraphe 1 est remplacé par le texte suivant:

«1. Les États membres exigent d'un marché réglementé qu'il développe sa résilience opérationnelle conformément aux exigences énoncées au chapitre II du règlement (UE) 2021/xx [DORA] pour garantir que ses systèmes de négociation sont résilients, possèdent une capacité suffisante pour gérer les volumes les plus élevés d'ordres et de messages, sont en mesure d'assurer un processus de négociation ordonné en période de graves tensions sur les marchés, sont soumis à des tests exhaustifs afin de confirmer que ces conditions sont réunies et sont régis par des mécanismes de continuité des activités assurant le maintien de ses services en cas de défaillance de ses systèmes de négociation.»

(b) Le paragraphe 6 est remplacé par le texte suivant:

«6. Les États membres exigent d'un marché réglementé qu'il dispose de systèmes, de procédures et de mécanismes efficaces, y compris qu'il exige de ses membres ou de ses participants qu'ils procèdent à des essais appropriés d'algorithmes et mettent à disposition les environnements facilitant ces essais conformément aux exigences énoncées aux chapitres II et IV du règlement (UE) 2021/xx [DORA], pour garantir que les systèmes de trading algorithmique ne donnent pas naissance ou ne contribuent pas à des conditions de négociation de nature à perturber le bon ordre du marché, et pour gérer les conditions de négociation de nature à perturber le bon ordre du marché qui découlent de ces systèmes de trading algorithmique, y compris de systèmes permettant de limiter la proportion d'ordres non exécutés par rapport aux transactions susceptibles d'être introduites dans le système par un membre ou un participant, de ralentir le flux d'ordres si le système risque d'atteindre sa capacité maximale ainsi que de limiter le pas minimal de cotation sur le marché et de veiller à son respect.»

(c) Le paragraphe 12 est modifié comme suit:

i) Le point a) est remplacé par le texte suivant:

«a) les exigences pour s'assurer que les systèmes de négociation des marchés réglementés sont résilients et disposent de capacités adéquates, à l'exception des exigences relatives à la résilience opérationnelle numérique;»

ii) Le point g) est remplacé par le texte suivant:

«g) les exigences pour veiller à l'essai approprié des algorithmes, autres que les essais en matière de résilience opérationnelle numérique, de manière à garantir que les systèmes de trading algorithmique, y compris les systèmes de trading algorithmique de haute fréquence, ne donnent pas naissance ou ne contribuent pas à des conditions de négociation de nature à perturber le bon ordre du marché.»

Article 7

Modifications de la directive (UE) 2015/2366

La directive (UE) 2015/2366 est modifiée comme suit:

(7) À l'article 5, paragraphe 1, troisième alinéa, la première phrase est remplacée par le texte suivant:

«La description des mesures de maîtrise et d'atténuation des risques en matière de sécurité visée au premier alinéa, point j), indique comment ces mesures garantissent un niveau élevé de sécurité technique et de protection des données, y compris pour les systèmes logiciels et informatiques utilisés par le demandeur ou par les entreprises vers lesquelles il externalise la totalité ou une partie de ses activités, conformément au chapitre II du règlement (UE) 2021/xx du Parlement européen et du Conseil * [DORA]. Ces mesures incluent également les mesures de sécurité prévues à l'article 95, paragraphe 1. Elles tiennent compte des orientations de l'ABE relatives aux mesures de sécurité, visées à l'article 95, paragraphe 3, une fois celles-ci établies.» _____

* [titre complet] (JO L […] du […], p. […]).

(8) L'article 95 est modifié comme suit:

(a) Le paragraphe 1 est remplacé par le texte suivant:

«1. Les États membres veillent à ce que les prestataires de services de paiement établissent un cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent; ce cadre prévoit que les prestataires de services de paiement établissent et maintiennent des procédures efficaces de gestion des incidents, y compris pour la détection et la classification des incidents opérationnels et de sécurité majeurs, tout en traitant les risques liés aux technologies de l'information et de la communication conformément au chapitre II du règlement (UE) 2021/xx [DORA].»

(b) Le paragraphe 4 est supprimé;

(c) Le paragraphe 5 est remplacé par le texte suivant:

«5. L'ABE encourage la coopération, y compris l'échange d'informations, dans le domaine des risques opérationnels associés aux services de paiement entre les autorités compétentes, et entre les autorités compétentes et la BCE.»

(9) L'article 96 est modifié comme suit:

(a) Le paragraphe 1 est remplacé par le texte suivant:

«1. En cas d'incident opérationnel ou de sécurité majeur qui n'est pas un incident informatique tel que défini à l'article 3, paragraphe 6, du règlement (UE) xx/20xx [DORA], le prestataire de services de paiement informe sans retard injustifié l'autorité compétente dans son État membre d'origine.»

(b) Le paragraphe 5 est supprimé;

(10) À l'article 98, le paragraphe 5 est remplacé par le texte suivant:

«5. Conformément à l'article 10 du règlement (UE) nº 1093/2010, l'ABE réexamine et, le cas échéant, met à jour les normes techniques de réglementation à intervalles réguliers, afin notamment de tenir compte de l'innovation et des progrès technologiques, ainsi que des dispositions du chapitre II du règlement (UE) 2021/xx [DORA].»

Article 8

Modification de la directive (UE) 2016/2341

À l'article 21, paragraphe 5, de la directive (UE) 2016/2341, la deuxième phrase est remplacée par le texte suivant:

«À cette fin, les IRP utilisent des systèmes, des ressources et des procédures appropriés et proportionnés, mettent en place des systèmes et des outils informatiques et gèrent ceux-ci conformément à l'article 6 du règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA].

_____

* [*titre complet*] (JO L […] du […], p. […]).»

Article 9

Transposition

1. Les États membres adoptent et publient, au plus tard le [un an après l'adoption], les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils communiquent immédiatement à la Commission le texte de ces dispositions.

   Ils appliquent ces dispositions à compter du [date d'entrée en vigueur de DORA/sa date d'application, si elle est différente].

   Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine couvert par la présente directive.

Article 10

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne.*

Article 11

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*