AVIS DE LA BANQUE CENTRALE EUROPÉENNE

du 11 avril 2022

sur une proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Introduction et fondement juridique

Le 16 décembre 2020, la Commission européenne a adopté une proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 ([1]) (ci-après la « directive proposée »). Le 3 décembre 2021, le Conseil de l'Union européenne a arrêté son orientation générale sur la directive proposée ([2]). La Banque centrale européenne (BCE) a compétence pour émettre un avis en vertu de l'article 127, paragraphe 4, deuxième alinéa, du traité sur le fonctionnement de l'Union européenne, étant donné que la directive proposée contient des dispositions relevant des domaines de compétence de la BCE, notamment la promotion du bon fonctionnement des systèmes de paiement, la contribution à la bonne conduite des politiques menées par les autorités compétentes en ce qui concerne la stabilité du système financier et les missions de la BCE ayant trait à la surveillance prudentielle des établissements de crédit en vertu de l'article 127, paragraphe 2, quatrième tiret, et paragraphes 5 et 6, du traité. Conformément à l'article 17.5, première phrase, du règlement intérieur de la Banque centrale européenne, le présent avis a été adopté par le conseil des gouverneurs.

Observations générales

La BCE soutient fermement les objectifs de la directive proposée visant à accroître le niveau de cyber-résilience dans tous les secteurs concernés, à réduire les incohérences dans l'ensemble du marché intérieur et à améliorer le niveau de prise de conscience de la situation et la capacité collective à se préparer et à réagir en assurant une coopération efficace dans l'Union.

La BCE reconnaît qu'il importe de maintenir des liens étroits entre la directive proposée et le secteur financier, qui devrait continuer à faire partie de l'écosystème des réseaux et des systèmes d'information (SRI) afin de promouvoir l'évaluation cohérente des risques liés aux technologies de l'information et de la communication (TIC) dans l'ensemble de l'Union et de favoriser un échange d'informations et une collaboration intersectoriels efficaces pour faire face aux cybermenaces. À cette fin, les autorités compétentes au titre de la proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier ([3]) (ci-après « le règlement sur la résilience opérationnelle numérique du secteur financier ») devraient pouvoir participer aux discussions stratégiques et aux travaux techniques du groupe de coopération SRI, ainsi qu'échanger des informations et coopérer davantage avec les points de contact uniques et les équipes nationales d'intervention en cas d'incidents de sécurité informatique (*Computer Security Incident Response Teams* – CSIRT) visés dans la directive proposée ([4]).

1. Champ d'application de la directive proposée

1.1 La BCE comprend qu'en ce qui concerne les entités du secteur financier, le règlement sur la résilience opérationnelle numérique du secteur financier sera considéré comme une législation sectorielle introduisant des exigences en matière de gestion des risques de cybersécurité et de notification des incidents qui soient au moins équivalentes, dans leurs effets, à celles prévues dans la directive proposée ([5]). Par conséquent, les dispositions de la directive proposée relatives à la gestion des risques de cybersécurité, aux obligations de signalement, au partage d'informations, à la surveillance et à l'exécution ne s'appliqueront pas aux entités financières couvertes par DORA ([6]). Comme précisé dans les considérants de la directive proposée, les dispositions du règlement sur la

([1]) COM(2020) 823 final.
([2]) Disponible sur le site internet du Conseil à l'adresse suivante : www.consilium.europa.eu.
([3]) COM(2020) 595 final.
([4]) Voir le paragraphe 1.5 de l'avis CON/2021/20 de la Banque centrale européenne du 4 juin 2021 sur une proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (JO C 343 du 26.8.2021, p. 1). Tous les avis de la BCE sont publiés sur EUR-Lex. Article 17, paragraphe 5, et article 42 du règlement sur la résilience opérationnelle numérique du secteur financier ; article 11 de la directive proposée.
([5]) Article 2, paragraphe 6, de la directive proposée.
([6]) Considérant 13 et article 2, paragraphe 6, de la directive proposée.

résilience opérationnelle numérique du secteur financier portant sur les mesures de gestion des risques concernant les TIC, la gestion des risques liés aux TIC et le signalement des incidents, le test de la résilience opérationnelle numérique, les accords de partage d'informations et les risques liés aux tiers en matière de TIC devraient s'appliquer au lieu de celles prévues par la directive proposée ([7]).

1.2 La BCE note également que le Conseil, dans son orientation générale sur la directive proposée, propose une modification visant à exclure du champ d'application de la directive proposée les « entités qui exercent des activités dans les domaines de la justice, des parlements ou des banques centrales » ([8]). La BCE comprend que la modification proposée s'étendrait à toutes les missions et compétences fondamentales du Système européen de banques centrales (SEBC), telles que définies à l'article 127, paragraphe 2, du traité et à l'article 3.1 des statuts du Système européen de banques centrales et de la Banque centrale européenne (ci-après les « statuts du SEBC »), telle que la promotion du bon fonctionnement des systèmes de paiement. À cet égard, les infrastructures des marchés financiers détenues et exploitées par l'Eurosystème, telles que TARGET2 et TARGET2-Titres, sont considérées comme relevant de la proposition du Conseil d'exclure les banques centrales de l'application de la directive proposée.

2. **Compétences dans le domaine de la surveillance du SEBC et de l'Eurosystème**

2.1 Outre l'objectif principal du SEBC, qui est de maintenir la stabilité des prix, et conformément à l'article 127, paragraphe 2, du traité, l'une des missions fondamentales relevant du SEBC est de promouvoir le bon fonctionnement des systèmes de paiement ([9]). Dans l'exécution de cette mission fondamentale, « la BCE et les banques centrales nationales peuvent accorder des facilités, et la BCE peut arrêter des règlements, en vue d'assurer l'efficacité et la solidité des systèmes de compensation et de paiements au sein de l'Union et avec les pays tiers » ([10]). Dans l'exercice de son rôle de surveillance, la BCE a adopté le règlement de la Banque centrale européenne (UE) n° 795/2014 (BCE/2014/28) ([11]) (ci-après le « règlement SPIS »), qui transpose les principes du CSPR-OICV pour les infrastructures de marchés financiers ([12]) en droit directement applicable. Le règlement SPIS fixe des exigences pour les systèmes de paiement de gros montants et les systèmes de paiement de détail d'importance systémique, qu'ils soient publics ou privés. Les exigences du règlement SPIS comprennent déjà, entre autres, la gestion des risques opérationnels et la mise en place d'un cadre de cyber-résilience ([13]).

2.2 Outre les systèmes de paiement d'importance systémique, la surveillance de l'Eurosystème couvre les systèmes de paiement d'importance non systémique, les instruments, systèmes et dispositifs de paiement électronique, ainsi que d'autres infrastructures et prestataires de services critiques, comme le prévoit le cadre de surveillance de l'Eurosystème ([14]). Les systèmes de paiement et autres dispositifs soumis à la surveillance de l'Eurosystème ne sont pas expressément inclus dans le champ d'application de la directive proposée ([15]). Dans le même temps, étant donné que la directive proposée est un instrument d'harmonisation minimale ([16]), la législation de mise en œuvre adoptée par les États membres pourrait, à terme, empiéter sur la compétence de l'Eurosystème en matière de surveillance. Pour éviter cela, les compétences du SEBC en vertu du traité et des statuts du SEBC, ainsi que les compétences de l'Eurosystème au titre du règlement SPIS et, de manière générale, du cadre de surveillance de l'Eurosystème, devraient être expressément reconnues dans les considérants de la directive proposée.

([7]) Considérant 13 de la directive proposée.
([8]) Article 2, paragraphe 3 *bis*, point 1), b), de l'orientation générale du Conseil sur la directive proposée.
([9]) Article 127, paragraphe 2, du TFUE, tel que repris à l'article 3.1 des statuts du SEBC.
([10]) Article 22 des statuts du SEBC.
([11]) Règlement (UE) n° 795/2014 de la Banque centrale européenne du 3 juillet 2014 concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique (BCE/2014/28) (JO L 217 du 23.7.2014, p. 16).
([12]) Voir le Comité sur les systèmes de paiement et de règlement (CSPR) et le Comité technique de l'Organisation internationale des commissions de valeurs (OICV), *Principes pour les infrastructures des marchés financiers*, avril 2012, disponibles sur le site internet de la Banque des règlements internationaux à l'adresse suivante : www.bis.org. La responsabilité D indique que « tous les membres du CSPR et de l'OICV devraient appliquer les principes aux IMF concernées dans leur juridiction dans la plus grande mesure permise par le cadre juridique ».
([13]) Article 15 du règlement (UE) n° 795/2014 (BCE/2014/28).
([14]) Cadre de surveillance de l'Eurosystème (*Eurosystem oversight policy framework*), version révisée (juillet 2016), disponible en anglais sur le site internet de la BCE à l'adresse suivante : www.ecb.europa.eu.
([15]) Article 2 et annexes I et II de la directive proposée.
([16]) Article 3 de la directive proposée.

3. **Risques liés aux tiers prestataires de services informatiques, gestion des crises et incidents majeurs, partage d'informations et stratégie nationale en matière de cybersécurité**

3.1 *Gestion des risques liés aux tiers prestataires de services informatiques*

3.1.1 La directive proposée habilite les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles, à émettre des instructions contraignantes ou une injonction exigeant de ces entités qu'elles remédient aux insuffisances constatées ou aux violations des obligations énoncées dans la directive proposée ([17]). Dans le même temps, le « superviseur principal » désigné en vertu du règlement sur la résilience opérationnelle numérique du secteur financier peut formuler des recommandations aux tiers prestataires critiques de services informatiques afin qu'ils gèrent les risques systémiques potentiels induits par les pratiques d'externalisation et par la concentration des dépendances à l'égard des tiers prestataires de services informatiques ([18]).

3.1.2 Étant donné qu'une entité essentielle au titre de la directive proposée peut également être désignée comme tiers prestataire critique de services informatiques en vertu du règlement sur la résilience opérationnelle numérique du secteur financier, la BCE rappelle ([19]) qu'il convient d'éviter de formuler des recommandations et des instructions contraignantes contradictoires. À cet égard, la BCE se félicite de l'orientation générale du Conseil sur la directive proposée. Selon cette approche, les autorités compétentes doivent informer le « forum de supervision », établi dans le cadre du règlement sur la résilience opérationnelle numérique du secteur financier, lorsqu'elles exercent leurs pouvoirs de surveillance et d'exécution à l'égard d'une entité essentielle désignée comme tiers prestataire critique de services informatiques dans le cadre du règlement sur la résilience opérationnelle numérique du secteur financier ([20]).

3.2 *Gestion des crises et incidents majeurs*

3.2.1 Conformément à la directive proposée ([21]), les États membres doivent désigner une ou plusieurs autorités compétentes chargées de la gestion des crises et incidents majeurs. Comme le précisent les considérants de la directive proposée, un incident majeur signifie un incident qui frappe plusieurs États membres ou qui provoque des perturbations dépassant les capacités d'action du seul État membre concerné. Les incidents majeurs peuvent se transformer en crises à part entière, empêchant le bon fonctionnement du marché intérieur ([22]).

3.2.2 Si les autorités compétentes désignées dans le cadre du règlement sur la résilience opérationnelle numérique du secteur financier restent responsables de la gestion des incidents de cybersécurité concernant des entités financières, la coopération avec les structures et autorités établies en vertu de la directive proposée sera essentielle pour assurer une réaction coordonnée dans l'ensemble de l'Union. À cette fin, la BCE accueillerait favorablement la participation des autorités compétentes désignées dans le cadre du règlement sur la résilience opérationnelle numérique du secteur financier, y compris la BCE, au réseau européen pour la préparation et la gestion des crises cyber (*Cyber Crises Liaison Organisation Network* – EU-CyCLONe) ([23]), lorsque des crises et incidents majeurs de cybersécurité touchent le secteur financier.

3.3 *Partage d'informations*

3.3.1 Comme indiqué ci-dessus, la BCE soutient fermement la coopération entre les autorités compétentes désignées dans le cadre du règlement sur la résilience opérationnelle numérique du secteur financier et les structures et autorités établies en vertu de la directive proposée. En particulier, le partage d'informations entre les autorités peut permettre un apprentissage intersectoriel, contribuer à la prévention et à la gestion efficace des cyberattaques et promouvoir l'évaluation cohérente des risques liés aux TIC dans l'ensemble de l'Union. Néanmoins, la BCE souligne que l'échange d'informations devrait avoir lieu lorsqu'il existe des mécanismes de classification et d'échange d'informations clairement établis et assortis de garanties de confidentialité adéquates ([24]). La BCE se félicite de

([17]) Article 29, paragraphe 4, point b), de la directive proposée.
([18]) Article 31 du règlement sur la résilience opérationnelle numérique du secteur financier.
([19]) Voir point 1.2 de l'avis CON/2021/20.
([20]) Article 29, paragraphe 10, de l'orientation générale du Conseil sur la directive proposée.
([21]) Article 7, paragraphe 1, de la directive proposée.
([22]) Considérant 27 de la directive proposée.
([23]) Article 14 de la directive proposée.
([24]) Voir point 1.5 de l'avis CON/2021/20.

l'orientation générale du Conseil sur la directive proposée qui propose l'échange régulier d'informations pertinentes entre les autorités ([25]), la mise en place d'arrangements de coopération précisant un mécanisme d'échange des informations ([26]) et la transmission automatique et directe des signalements d'incidents ([27]). À cet égard, il convient de veiller à ce que les informations qui sont confidentielles conformément aux dispositions relatives au secret professionnel prévues par le règlement sur la résilience opérationnelle numérique du secteur financier ([28]) ou par la législation sectorielle concernée ([29]) ne puissent être échangées avec les autorités compétentes visées dans la directive proposée que si cet échange est nécessaire à l'application des dispositions de la directive proposée par les autorités compétentes ([30]).

3.4 *Stratégie nationale en matière de cybersécurité*

3.4.1 En vertu de la directive proposée, les États membres sont tenus d'adopter des stratégies nationales en matière de cybersécurité qui définissent les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir ([31]). Comme précisé dans les considérants de la directive proposée, les États membres devraient continuer de couvrir le secteur financier dans leurs stratégies respectives de cybersécurité ([32]). À titre indicatif, dans le cadre de leurs stratégies nationales de cybersécurité, les États membres devraient adopter des politiques traitant de la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par les entités pour la fourniture de leurs services. En ce qui concerne le secteur financier, les stratégies nationales de cybersécurité devraient être cohérentes avec le cadre réglementaire qui émane du règlement sur la résilience opérationnelle numérique du secteur financier. À cet égard, la BCE estime que des éclaircissements supplémentaires sont nécessaires pour garantir la cohérence des stratégies nationales de cybersécurité avec la législation sectorielle.

Pour toute recommandation quant à une modification de la directive proposée, la BCE propose un libellé spécifique dans un document de travail technique distinct, accompagné d'un texte explicatif à cet effet. Le document de travail technique peut être consulté en anglais sur EUR-Lex.

Fait à Francfort-sur-le-Main, le 11 avril 2022.

La présidente de la BCE
Christine LAGARDE

([25]) Article 11, paragraphe 5, de l'orientation générale du Conseil sur la directive proposée.
([26]) Considérant 23 *bis* de l'orientation générale du Conseil sur la directive proposée.
([27]) Considérant 13 de l'orientation générale du Conseil sur la directive proposée.
([28]) Article 49 du règlement sur la résilience opérationnelle numérique du secteur financier
([29]) Articles 53 à 62 de la directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 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 (JO L 176,du 27.6.2013, p. 338)
([30]) Article 2, paragraphe 5, et article 11, paragraphe 4, de la directive proposée.
([31]) Article 5 de la directive proposée.
([32]) Considérant 13 de la directive proposée.