III

(Actes préparatoires)

BANQUE CENTRALE EUROPÉENNE

AVIS DE LA BANQUE CENTRALE EUROPÉENNE

du 25 juillet 2014

sur une proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

(CON/2014/58)

(2014/C 352/04)

Introduction et fondement juridique

Le 7 février 2013, la Commission européenne a publié une proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union ([1]) (ci-après la «directive proposée»).

N'ayant pas été consultée formellement par les législateurs, la Banque centrale européenne (BCE) a décidé d'émettre un avis, de sa propre initiative, sur la directive proposée. La BCE a compétence pour émettre un avis en vertu de l'article 127, paragraphe 4, et de l'article 282, paragraphe 5, du traité sur le fonctionnement de l'Union européenne, étant donné que la directive proposée contient des dispositions ayant une incidence sur les missions du Système européen de banques centrales (SEBC) consistant à promouvoir le bon fonctionnement des systèmes de paiement visé à l'article 127, paragraphe 2, quatrième tiret, du traité. De plus, l'article 22 des statuts du Système européen de banques centrales et de la Banque centrale européenne (ci-après les «statuts du SEBC») mentionne que la BCE et les banques centrales nationales (BCN) peuvent accorder des facilités et la BCE peut arrêter des réglements en vue d'assurer l'efficacité et la solidité des systèmes de compensation et de paiement au sein de l'Union et avec les pays tiers. 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.

1. Objet de la directive proposée

1.1 La directive proposée vise à assurer un niveau commun élevé de sécurité des réseaux et de l'information (SRI) en améliorant la sécurité de l'internet et des réseaux et systèmes informatiques sur lesquels reposent notre société et l'économie. Cette proposition constitue la principale mesure prise dans le cadre de la stratégie de cybersécurité de l'Union européenne ([2]),

1.2 Les réseaux et systèmes informatiques jouent un rôle essentiel dans la circulation transfrontalière des biens, des services et des personnes. Du fait de leur dimension transnationale intrinsèque, toute perturbation de ces systèmes dans un État membre peut avoir également une incidence sur d'autres États membres et sur l'Union dans son ensemble. De plus, la probabilité que de tels incidents se produisent fréquemment à l'avenir et l'incapacité d'assurer une protection efficace mine la confiance du public à l'égard de la SRI. La résilience et la stabilité de la SRI sont donc capitales pour le fonctionnement harmonieux du marché intérieur.

1.3 La directive proposée s'inscrit dans la continuité de précédentes initiatives dans ce domaine ([3]). Dans ce contexte, la directive proposée reconnaît le besoin d'harmoniser les règles relatives à la SRI et de créer des mécanismes de coopération efficaces entre les États membres.

([1]) COM(2013) 48 final.

([2]) Voir la communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions: «Un cyberespace ouvert, sûr et sécurisé», JOIN(2013) 1 final.

([3]) Ces initiatives incluent les communications suivantes: «Sécurité des réseaux et de l'information: proposition pour une approche politique européenne» COM(2001) 298 final; «Une stratégie pour une société de l'information sûre: "Dialogue, partenariat et responsabilisation"» COM(2006) 251 final; «Protection des infrastructures d'information critiques – "Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité et la résilience"» COM(2009) 149 final; «Une stratégie numérique pour l'Europe» COM(2010) 245 final; et «Protection des infrastructures d'information critiques – "Réalisations et prochaines étapes: vers une cybersécurité mondiale"» COM(2011) 163 final.

1.4 La directive proposée établit un cadre juridique commun à l'Union pour la SRI concernant les capacités des États membres, les mécanismes de coopération au niveau de l'Union et les obligations des administrations publiques et des entités du secteur privé dans les secteurs définis comme critiques. Ce cadre doit garantir une préparation adéquate au niveau national et aider à susciter un climat de confiance mutuelle, ce qui est une condition préalable à une coopération effective au niveau de l'Union. L'instauration de mécanismes de coopération au niveau de l'Union par le biais du réseau fournira des moyens cohérents et coordonnés de prévention et de réaction face aux incidents et risques transfrontaliers en matière de SRI.

1.5 Les principales mesures concernent les aspects suivants:

a) l'obligation, pour tous les États membres, de mettre en place un minimum de moyens au niveau national en établissant des autorités compétentes dans le domaine de la SRI, en instaurant des équipes d'intervention en cas d'urgence informatique (CERT) et en adoptant des stratégies et des plans de coopération nationaux en matière de SRI;

b) l'obligation du partage de l'information entre les États membres au sein d'un réseau, ainsi que la mise en place d'un plan européen de coopération en matière de SRI et des alertes précoces coordonnées pour signaler les incidents de cybersécurité;

c) la garantie, sur le modèle de la directive 2002/21/CE du Parlement européen et du Conseil ([1]), du développement d'une culture de la gestion du risque et du partage des informations entre les secteurs public et privé. Les entreprises des secteurs définis comme critiques et les administrations publiques devront évaluer les risques qu'elles courent et adopter des mesures appropriées et proportionnées pour garantir la SRI. Elles seront également tenues de signaler aux autorités compétentes tout incident qui compromet sérieusement leurs réseaux et leurs systèmes informatiques et qui a une incidence significative sur la continuité des services critiques et l'approvisionnement des biens.

2. **Observations d'ordre général**

2.1 La BCE soutient l'objectif de la directive proposée de garantir un niveau commun élevé de SRI à travers l'Union et de parvenir à une cohérence d'approche en la matière dans tous les secteurs d'activité et tous les États membres. Il est important de veiller à ce que le marché intérieur soit un lieu sûr pour exercer des activités et que tous les États membres disposent d'un certain niveau minimal de préparation en cas de survenance d'un incident de cybersécurité.

2.2 Toutefois, la BCE considère que la directive proposée ne doit pas porter préjudice au cadre existant en matière de surveillance des systèmes de paiement et de règlement de l'Eurosystème ([2]) qui comprend des dispositifs appropriés, notamment dans le domaine de la SRI. Il convient de noter que la BCE a un intérêt particulier à une sécurité accrue des systèmes de paiement et de règlement ([3]) de manière à promouvoir le bon fonctionnement des systèmes de paiement et à contribuer au maintien de la confiance dans l'euro et dans le fonctionnement de l'économie de l'Union.

2.3 De plus, l'évaluation des dispositifs de sécurité et des notifications d'incident des systèmes de paiement et de règlement et des prestataires de services de paiement (PSP) constitue l'une des compétences fondamentales des autorités de surveillance prudentielle et des banques centrales. La responsabilité de l'élaboration d'obligations en matière de surveillance dans les domaines mentionnés ci-dessus doit donc rester celle de ces autorités et les systèmes de paiement et de règlement et les PSP ne doivent pas être soumis à d'éventuelles obligations contradictoires imposées par d'autres autorités nationales. De plus, la gestion du risque, y compris les obligations en matière de sécurité concernant les systèmes de paiement et de règlement et d'autres infrastructures de marché au sein de la zone euro, est définie par l'Eurosystème qui englobe la BCE et les BCN des États membres qui ont adopté l'euro. Par le biais de cette fonction de surveillance, l'Eurosystème vise à garantir le bon fonctionnement des systèmes de paiement et de règlement en appliquant, entre autres, des normes de surveillance adéquates et des exigences minimales. La directive proposée doit tenir compte du cadre de surveillance déjà en place et garantir la cohérence réglementaire au sein de l'Union.

3. **Remarques particulières**

3.1 Le considérant 5 et l'article 1er de la directive proposée prévoient que les obligations pertinentes, le mécanisme de coopération et les exigences en matière de sécurité s'appliquent à l'ensemble des administrations publiques et des acteurs du marché. Le libellé actuel du considérant 5 et de l'article 1er ne tient pas compte de la mission conférée à l'Eurosystème, et figurant dans le traité, consistant à assurer la surveillance des systèmes de paiement et de règlement. Il convient par conséquent de modifier la directive proposée de manière à refléter correctement les responsabilités de l'Eurosystème dans ce domaine.

([1]) Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (JO L 108 du 24.4.2002, p. 33).

([2]) Les fonctions de surveillance de certains membres du SEBC sont assurées sur la base des lois et des règlements nationaux qui complètent, et dans certains cas chevauchent, la compétence de l'Eurosystème.

([3]) Dans l'ensemble du présent avis, l'emploi du terme «règlement» inclut la fonction de compensation.

3.2 Les dispositifs et procédures sur lesquels les banques centrales et les autres autorités compétentes s'appuient pour assurer la surveillance des systèmes de paiement et de règlement des opérations sur titres figurent dans un certain nombre de règlements et directives de l'Union, parmi lesquels:

a) la directive 98/26/CE du Parlement européen et du Conseil ([1]) (ci-après la «directive concernant le caractère définitif du règlement»), qui autorise les autorités compétentes des États membres à imposer aux systèmes de paiement et de règlement relevant de leur juridiction des dispositifs en matière de surveillance prudentielle ([2]);

b) le règlement (UE) nº 648/2012 du Parlement européen et du Conseil ([3]) [ci-après le «règlement européen des infrastructures de marché» (EMIR)], qui reconnaît les fonctions respectives de l'Autorité européenne des marchés financiers (AEMF), de l'Autorité bancaire européenne (ABE) et du SEBC en matière de définition des normes réglementaires et de surveillance prudentielle des contreparties centrales; et

c) la proposition de règlement portant sur l'amélioration du règlement des opérations sur titres dans l'Union européenne et sur les dépositaires centraux de titres (DCT) et modifiant la directive 98/26/CE ([4]) [ci-après le «règlement DCT» (RDCT)], qui oblige à investir les autorités compétentes de pouvoirs de surveillance prudentielle et d'enquête, et en particulier l'article 45 de ce règlement, qui introduit des obligations prudentielles applicables aux DCT, ainsi que d'importantes mesures relatives à l'atténuation du risque opérationnel.

3.3 De plus, il convient de noter que le conseil des gouverneurs de la BCE a adopté, le 3 juin 2013, les «principes pour les infrastructures de marchés financiers» introduits en avril 2012 par le comité sur les systèmes de paiement et de règlement (CSPR) de la Banque des règlements internationaux et le comité technique de l'Organisation internationale des commissions de valeur (OICV) ([5]) aux fins de la surveillance, par l'Eurosystème, de tous les types d'infrastructures de marchés financiers. À cette étape a succédé une consultation publique concernant un projet de règlement relatif aux obligations de surveillance des systèmes de paiement d'importance systémique (ci-après le «règlement SPIS») ([6]). Le règlement SPIS met en œuvre les principes du CSPR-OICV d'une manière juridiquement contraignante et porte sur les systèmes de paiement (tant de montants élevés que de détail) d'importance systémique, qu'ils soient exploités par des BCN de l'Eurosystème ou par des entités privées.

3.4 Les dispositifs existant en matière de surveillance ([7]) en ce qui concerne les systèmes de paiement et les PSP prévoient déjà des procédures d'alerte précoces ([8]) et des réactions coordonnées ([9]) à l'intérieur et hors de l'Eurosystème pour traiter d'éventuelles menaces en matière de cybersécurité, semblables à celles définies aux articles 10 et 11 de la directive proposée.

3.5 Le SEBC a fixé des normes relatives aux obligations de déclaration et de gestion du risque pour les systèmes de paiement. De plus, la BCE évalue régulièrement les systèmes de règlement des opérations sur titres de manière à déterminer leur éligibilité aux opérations de crédit de l'Eurosystème. Par conséquent, la BCE considère qu'il est nécessaire que les obligations figurant dans la directive proposée concernant les infrastructures de marché essentielles et leurs opérateurs ([10]) ne portent pas atteinte aux normes du règlement SPIS, au cadre de politique de surveillance de l'Eurosystème ou à d'autres règlements de l'Union, et en particulier EMIR et à l'avenir le règlement DCT . De plus, elles ne doivent pas interférer avec les missions de l'ABE ou de l'AEMF, ni avec celles d'autres autorités de surveillance prudentielle ([11]).

([1]) Directive 98/26/EC du Parlement européen et du Conseil du 19 mai 1998 concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres (JO L 166 du 11.6.1998, p. 45).
([2]) Voir l'alinéa 3 de l'article 10, paragraphe 1, de la directive sur le caractère définitif du règlement.
([3]) Règlement (UE) nº 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (JO L 201 du 27.7.2012, p. 1).
([4]) COM(2012) 73 final.
([5]) Disponible sur le site internet de la Banque des règlements internationaux à l'adresse suivante: https://www.bis.org/publ/cpss94.pdf
([6]) Disponible sur le site internet de la BCE à l'adresse suivante: http://www.ecb.europa.eu
([7]) Voir le communiqué de presse de la BCE concernant le *Memorandum of Understanding (MoU) on high-level principles of co-operation between the banking supervisors and central banks of the European Union in crisis management situations* (2003) (Protocole d'accord sur les principes de coopération à un niveau élevé entre les autorités de contrôle bancaire et les banques centrales de l'Union européenne dans les situations de gestion de crise, 2003), disponible sur le site internet de la BCE à l'adresse suivante: www.ecb.europa.eu
([8]) Voir recommandation 3: le suivi et la déclaration des incidents dans les recommandations intitulées *«Recommendations for the security of internet payments-final version after public consultation»* (Recommandations relatives à la sécurité des paiements sur internet – version finale après consultation publique), *The European Forum on the Security of Retail Payments (SecuRe Pay)* [Le forum européen sur la sécurité des paiements de détail (SecuRe Pay)], janvier 2013, disponible sur le site internet de la BCE à l'adresse suivante: www.ecb.europa.eu
([9]) Sur la base des principes de coopération internationale en matière de surveillance, réaffirmés par le CSPR dans son rapport de 2005 sur la surveillance, les banques centrales de l'Eurosystème ont participé avec succès à des dispositifs concertés dans un certain nombre de cas, ainsi, par exemple, dans le contexte des dispositifs de surveillance concernant SWIFT [*Society for Worldwide Interbank Financial Telecommunications*, (Société pour les télécommunications financières interbancaires mondiales)] et concernant le système *Continuous Linked Settlement* (CLS).
([10]) Par exemple les exigences s'appliquant aux acteurs du marché à prendre des mesures techniques et organisationnelles mentionnées à l'article 14, paragraphes 3 et 4, et la compétence de donner des instructions contraignantes aux acteurs du marché mentionnée à l'article 15, paragraphe 3, de la directive proposée.
([11]) Voir point 2.12 de l'avis CON/2014/9 de la BCE sur une proposition de directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/UE et 2009/110/CE et abrogeant la directive 2007/64/CE (JO C 224 du 15.7.2014, p. 1). Tous les avis de la BCE sont publiés sur le site internet de la BCE à l'adresse suivante: www.ecb.europa.eu

3.6 Nonobstant ce qui précède, la BCE considère qu'il serait essentiel pour l'Eurosystème de partager les informations pertinentes avec le comité SRI à mettre en place conformément à l'article 19 de la directive proposée. Aux fins du partage effectif des informations qui peut s'avérer nécessaire, la BCE, l'ABE et l'AEMF devrait être invitées à envoyer des représentants aux réunions du comité SRI pour les points de l'ordre du jour pouvant être intéressants eu égard à l'exercice de leurs mandats respectifs.

Fait à Francfort-sur-le-Main, le 25 juillet 2014.

Le président de la Banque centrale européenne

Mario DRAGHI

ANNEXE

Suggestions de rédaction

Texte proposé par la Commission	Modifications proposées par la BCE [1]
Modification 1 Considérant 5	
«5) Pour que tous les incidents et risques pertinents soient couverts, il convient que la présente directive s'applique à tous les réseaux et systèmes informatiques. Les obligations imposées aux administrations publiques et aux acteurs du marché ne devraient cependant pas être applicables aux entreprises qui fournissent des réseaux de communication publics ou des services de communications électroniques accessibles au public au sens de la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre") [2], qui sont soumises aux dispositions particulières relatives à la sécurité et à l'intégrité énoncées à l'article 13 *bis* de ladite directive, ni aux fournisseurs de services de confiance.»	«5) Pour que tous les incidents et risques pertinents soient couverts, il convient que la présente directive s'applique à tous les réseaux et systèmes informatiques. Les obligations imposées aux administrations publiques et aux acteurs du marché ne devraient cependant pas être applicables aux entreprises qui fournissent des réseaux de communication publics ou des services de communications électroniques accessibles au public au sens de la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre") [2], qui sont soumises aux dispositions particulières relatives à la sécurité et à l'intégrité énoncées à l'article 13 *bis* de ladite directive, ni aux fournisseurs de services de confiance. **De plus, nonobstant l'application de la présente directive aux administrations publiques et aux acteurs du marché, la présente directive ne porte pas atteinte aux missions et devoirs conférés au Système européen de banques centrales (SEBC) par le traité et les statuts du Système européen de banques centrales et de la Banque centrale européenne, ni aux fonctions équivalentes assumées par des membres du SEBC en vertu de leurs cadres nationaux, notamment en ce qui concerne les politiques de surveillance prudentielle des établissements de crédit et la surveillance des systèmes de paiement et de règlement d'opérations sur titres. Les États membres s'appuient sur les fonctions de surveillance prudentielle et de surveillance exercées par les banques centrales et les autorités de surveillance prudentielle de ces opérateurs dans leurs champs de compétence.**»

Explication

Le considérant 5 doit être modifié de manière à refléter les responsabilités de la BCE et des BCN en matière de surveillance et de réglementation concernant les systèmes de paiement et de règlement. Conformément à l'article 127, paragraphe 2, quatrième tiret, du traité, l'une des missions fondamentales du SEBC consiste à promouvoir le bon fonctionnement des systèmes de paiement. L'article 22 des statuts du SEBC donne également compétence à la BCE pour arrêter des règlements en vue d'assurer l'efficacité et la solidité des systèmes de compensation et de paiement. Il convient de tenir compte du fait que, conformément à l'article 127, paragraphe 5, du traité, le SEBC contribue à la bonne conduite des politiques menées en ce qui concerne la stabilité du système financier. De plus, selon le cadre de surveillance de l'Eurosystème de juillet 2011 [2], la surveillance des systèmes de paiement et de règlement est une fonction de banque centrale dont les objectifs de sécurité et d'efficacité sont promus en effectuant un suivi des systèmes actuels et de ceux qui sont prévus, en procédant à leur évaluation au regard de ces objectifs et, le cas échéant, en provoquant des changements.

En d'autres termes, garantir la sécurité et l'efficacité des systèmes est une condition préalable essentielle pour que l'Eurosystème soit capable de contribuer à la stabilité financière, de mettre en œuvre la politique monétaire et de préserver la confiance du public dans l'euro.

De plus, conformément aux commentaires de la BCE sur la révision proposée de la directive sur les services de paiement (DSP2), il convient de noter que les autorités de surveillance prudentielle nationales et les banques centrales sont les autorités qui ont compétences pour émettre des lignes directrices relativement à la gestion et à la notification des incidents concernant les PSP, de même que pour émettre des lignes directrices relativement au partage d'informations relativement à la notification des incidents entre autorités compétentes. Le considérant devrait également tenir compte des missions confiées à la BCE par le règlement (UE) nº 1024/2013.

Texte proposé par la Commission	Modifications proposées par la BCE [1]
Enfin, lorsque des États membres du SEBC n'appartenant pas à la zone euro assument, dans le cadre de dispositions nationales, des fonctions équivalentes à celles du traité et aux missions mentionnées dans les statuts du SEBC, il ne doit pas non plus être porté atteinte à ces fonctions.	

Modification 2

Article 1, paragraphes 4 et 5 (nouveau)

«4. La présente directive ne porte pas atteinte aux dispositions de la législation de l'UE sur la cybercriminalité ni à celles de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection [9]	«4. La présente directive ne porte pas atteinte aux dispositions de la législation de l'U~~E~~**nion** sur la cybercriminalité ni à celles de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection [9].
5. Elle ne porte pas non plus atteinte aux dispositions de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [10], de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et du règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [11].	**5. La présente directive est sans préjudice de la surveillance et des missions confiées à la BCE et au SEBC ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit et aux systèmes de paiement et de règlement pour lesquels des exigences spécifiques en matière de gestion et de sécurité des risques ont été fixées dans le cadre réglementaire du SEBC et dans celui d'autres directives et règlements de l'Union connexes. De même, la présente directive ne porte pas atteinte aux fonctions équivalentes assumées par les membres du SEBC dans le cadre de leurs réglementations nationales.**
6. Le partage des informations au sein du réseau de coopération visé au chapitre III et les notifications d'incidents de SRI en vertu de l'article 14 peuvent nécessiter le traitement de données à caractère personnel. Ce traitement, qui est nécessaire à l'exécution de la mission d'intérêt public qui est celle de la présente directive, est autorisé par l'État membre conformément à l'article 7 de la directive 95/46/CE et à la directive 2002/58/CE, tels que transposés en droit national.»	~~5~~**6.** Elle ne porte pas non plus atteinte aux dispositions de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [10], de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et du règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [11]. ~~6~~**7.** Le partage des informations au sein du réseau de coopération visé au chapitre III et les notifications d'incidents de SRI en vertu de l'article 14 peuvent nécessiter le traitement de données à caractère personnel. Ce traitement, qui est nécessaire à l'exécution de la mission d'intérêt public qui est celle de la présente directive, est autorisé par l'État membre conformément à l'article 7 de la directive 95/46/CE et à la directive 2002/58/CE, tels que transposés en droit national.»

Explication

Comme mentionné ci-dessus, le SEBC a un intérêt tout particulier à assurer correctement cette fonction concernant les sytèmes de paiement et de règlement. Ceci résulte de l'importance des systèmes de paiement, de compensation et de règlement pour la bonne conduite des opérations de politique monétaire et de leur rôle dans la garantie de la stabilité du système financier en général. Par conséquent, la BCE recommande que la directive proposée tienne compte du rôle du SEBC en ce qui concerne les systèmes de paiement et de règlement et du cadre de surveillance déjà en place. Le SEBC dispose d'outils extrêmement performants pour déterminer les niveaux de sécurité et d'efficacité de ces systèmes. Le considérant doit tenir compte des missions confiées à la BCE par le règlement (UE) no 1024/2013.

La directive proposée ne porte pas atteinte aux fonctions équivalentes assumées par des membres du SEBC n'appartenant pas à la zone euro dans le cadre de dispositions nationales.

Texte proposé par la Commission	Modifications proposées par la BCE [1]

Modification 3

Article 6, paragraphe 1

«1. Chaque État membre désigne une autorité nationale compétente en matière de sécurité des réseaux et systèmes informatiques (l'"autorité compétente").»	«1. Chaque État membre désigne une autorité nationale compétente en matière de sécurité des réseaux et systèmes informatiques (l'"autorité compétente"). **Une coopération effective doit être instaurée entre l'autorité compétente et les autorités de réglementation nationales et européennes.**»

Explication

La BCE recommande de modifier l'article 6, paragraphe 1, de manière à garantir un bon niveau de coopération à l'échelle de l'Union.

Modification 4

Article 8, paragraphe 3

«3. Au sein du réseau de coopération, les autorités compétentes:	«3. Au sein du réseau de coopération, les autorités compétentes:
a) diffusent les messages d'alerte rapide sur les risques et incidents conformément à l'article 10;	a) diffusent les messages d'alerte rapide sur les risques et incidents conformément à l'article 10;
b) assurent une intervention coordonnée conformément à l'article 11;	b) assurent une intervention coordonnée conformément à l'article 11;
c) publient régulièrement, sur un site web commun, des informations non confidentielles sur les alertes rapides et les interventions coordonnées en cours;	c) publient régulièrement, sur un site web commun, des informations non confidentielles sur les alertes rapides et les interventions coordonnées en cours;
d) procèdent, à la demande d'un État membre ou de la Commission, à un examen et une évaluation communs d'un ou de plusieurs plans de coopération et stratégies nationaux en matière de SRI visés à l'article 5, dans le champ d'application de la présente directive;	d) procèdent, à la demande d'un État membre ou de la Commission, à un examen et une évaluation communs d'un ou de plusieurs plans de coopération et stratégies nationaux en matière de SRI visés à l'article 5, dans le champ d'application de la présente directive;
e) procèdent, à la demande d'un État membre ou de la Commission, à un examen et une évaluation communs de l'efficacité des CERT, notamment lorsque des exercices de SRI sont exécutés au niveau de l'Union;	e) procèdent, à la demande d'un État membre ou de la Commission, à un examen et une évaluation communs de l'efficacité des CERT, notamment lorsque des exercices de SRI sont exécutés au niveau de l'Union;
f) coopèrent et échangent des informations sur tous les aspects pertinents avec le Centre européen de lutte contre la cybercriminalité au sein d'Europol, et avec d'autres organismes européens concernés, notamment dans le domaine de la protection des données, de l'énergie, des transports, des services bancaires, des bourses de valeurs et de la santé;	f) coopèrent et échangent des informations sur tous les aspects pertinents avec le Centre européen de lutte contre la cybercriminalité au sein d'Europol, et avec d'autres organismes européens concernés, notamment dans le domaine de la protection des données, de l'énergie, des transports, des services bancaires, des bourses de valeurs et de la santé;
g) échangent des informations et de bonnes pratiques, entre elles et avec la Commission, et s'assistent mutuellement en ce qui concerne le renforcement des capacités de SRI;	g) échangent des informations et de bonnes pratiques, entre elles et avec la Commission, et s'assistent mutuellement en ce qui concerne le renforcement des capacités de SRI;
h) organisent régulièrement des examens par les pairs portant sur les moyens et l'état de préparation;	h) organisent régulièrement des examens par les pairs portant sur les moyens et l'état de préparation;

Texte proposé par la Commission	Modifications proposées par la BCE [1]
i) organisent des exercices de SRI au niveau de l'Union et participent, le cas échéant, à des exercices de SRI internationaux.»	i) organisent des exercices de SRI au niveau de l'Union et participent, le cas échéant, à des exercices de SRI internationaux**;** **j) garantissent l'échange des informations avec les autorités de régulation européennes et nationales [par exemple pour le secteur financier: le Système européen de banques centrales (SEBC), l'Autorité bancaire européenne (ABE) et l'Autorité européenne des marchés financiers (AEMF), qui coopèrent étroitement lorsque des incidents de sécurité susceptibles d'entraver le bon fonctionnement des systèmes de paiement et de règlement sont identifiés]**.»

Explication

Il est essentiel de partager les informations avec l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) ou avec les autorités compétentes dans le cadre de la directive proposée et avec l'ABE et l'AEMF en tant qu'autorité compétente pour la coordination lors d'incidents liés aux PSP.

Par conséquent la BCE propose cette modification dans le but d'encourager le partage des informations et d'améliorer la coordination au niveau européen.

Modification 5

Article 19, paragraphe 1

«1. La Commission est assistée par un comité (comité de la sécurité des réseaux et de l'information). Il s'agit d'un comité au sens du règlement (UE) nº 182/2011.»	«1. La Commission est assistée par un comité (comité de la sécurité des réseaux et de l'information). Il s'agit d'un comité au sens du règlement (UE) nº 182/2011. **La BCE, l'ABE et l'AEMF sont invitées à envoyer un réprésentant aux réunions du comité de la sécurité des réseaux et de l'information pour les points de l'ordre du jour qui pourraient avoir des conséquences sur l'exécution des mandats respectifs de la BCE, de l'ABE ou de l'AEMF.**»

Explication

La BCE a un intérêt tout particulier à renforcer la sécurité des systèmes, services et instruments de paiement et de règlement, qui constitue un élément important du maintien de la confiance dans la monnaie unique et dans le bon fonctionnement de l'économie de l'Union. À cette fin, la BCE recommande qu'elle soit invitée aux réunions du comité SRI. Dans tous les cas, la BCE devra être formellement consultée, conformément au traité, sur toutes les mesures liées aux systèmes de paiement et tous les autres aspects relevant des champs de compétence de la BCE.

L'ABE ou l'AEMF devraient également participer aux travaux sur les questions ayant trait aux PSP.

[1] Les caractères en gras dans le corps du texte indiquent les nouveaux passages suggérés par la BCE. Les caractères barrés dans le corps du texte indiquent les passages que la BCE propose de supprimer.

[2] Disponible sur le site de la BCE à l'adresse suivante: www.ecb.europa.eu