BANQUE CENTRALE EUROPÉENNE

EUROSYSTÈME

FR **ECB-PUBLIC**

AVIS DE LA BANQUE CENTRALE EUROPÉENNE

du 18 mai 2018

sur l'établissement d'un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

(CON/2018/27)

Introduction et fondement juridique

Le 18 avril 2018, la Banque centrale européenne (BCE) a reçu une demande de consultation de la part du ministre des finances belge portant sur un projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général (ci-après le « projet de loi »).

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, lus conjointement avec l'article 127, paragraphe 6, du traité et de l'article 2, paragraphe 1, troisième tiret, de la décision 98/415/CE du Conseil[1], étant donné que le projet de loi a trait à la Banque Nationale de Belgique (« BNB »), aux systèmes de paiement et de règlement, aux règles applicables aux établissements financiers dans la mesure où elles ont une incidence sensible sur la stabilité des établissements et marchés financiers et aux missions de la BCE relatives à la surveillance prudentielle des établissements de crédit. 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 du projet de loi

1.1 Le projet de loi a pour objet de transposer la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union[2] (ci-après la « directive NIS »), en tenant compte de l'article 1er, paragraphe 7, en vertu duquel des obligations équivalentes sont imposées par des actes juridiques sectoriels de l'Union aux opérateurs de services essentiels pour qu'ils assurent la sécurité de leurs réseaux et systèmes d'information ou qu'ils procèdent à la notification des incidents[3].

1.2 En particulier, la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques[4] (ci-après la « loi sur les infrastructures critiques »), qui a transposé la directive

1 Décision du Conseil 98/415/CE du 29 juin 1998 relative à la consultation de la Banque centrale européenne par les autorités nationales au sujet de projets de réglementation (JO L 189 du 3.7.1998, p. 42).

2 JO L 194 du 19.7.2016, p. 1.

3 Exposé des motifs du projet de loi, p. 6.

4 Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

2008/114/UE 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[5] a établi en Belgique un cadre complet applicable aux infrastructures critiques définies comme une installation, système ou partie de celui-ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions. Ces infrastructures critiques sont identifiées, désignées et suivies de près par des autorités sectorielles qui doivent veiller à ce que les exploitants adoptent et élaborent un plan de sécurité visant à prévenir, à atténuer et à neutraliser les risques d'interruption de leur fonctionnement ou de leur destruction. La BNB a été nommée en tant qu'autorité sectorielle pour le secteur financier.

1.3 Par souci de cohérence avec la loi sur les infrastructures critiques, les infrastructures critiques désignées par la BNB sont automatiquement considérées comme des opérateurs de services essentiels en vertu du projet de loi. En outre, toutes les dispositions du projet de loi selon lesquelles les autorités sectorielles peuvent soumettre les opérateurs de services essentiels à des obligations de sécurité, des audits interne et externe, des contrôles, des vérifications et des inspections s'appliquent à tous les secteurs, à l'exception du secteur financier. Les opérateurs de services essentiels relevant du champ d'application du secteur financier ne sont soumis qu'aux dispositions du projet de loi relatives aux notifications d'incidents et aux sanctions administratives. Tandis que la BNB agira, à cet effet, en tant qu'autorité sectorielle pour les établissements de crédit et les contreparties centrales, l'Autorité des services et marchés financiers agira en cette qualité pour les opérateurs de plateformes de négociation.

1.4 Le projet de loi prévoit également des mécanismes de coopération et/ou d'échange d'informations au niveau national et international. Au niveau national, cette coopération et cet échange d'informations, y compris pour les notifications d'incidents, ont lieu entre le Centre pour la Cybersecurité Belgique (CCB), la Direction générale Centre de Crise du Service public fédéral Intérieur (DGCC), les autorités sectorielles ainsi que, si besoin est, les services du Ministère public, la police et l'Autorité de protection des données belge. Au niveau international, l'échange d'informations a lieu avec des autorités de l'Union européenne et des autorités nationales ou étrangères lorsque cela est nécessaire à la mise en œuvre du projet de loi.

1.5 Le projet de loi modifie la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique[6] (ci-après la « loi organique de la BNB ») afin de fixer formellement la compétence de la BNB pour contrôler le respect par les opérateurs du secteur financier de ses dispositions, d'habiliter la Commission des sanctions à appliquer les sanctions administratives prévues et d'autoriser l'échange d'informations avec les autorités nationales compétentes pour la sécurité des réseaux et des systèmes d'information d'intérêt général.

5 JO L 345 du 23.12.2008, p. 75.

6 Loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique.

2. Observations générales

2.1 Le projet de loi transpose la directive NIS qui est, selon son article 3, une directive d'harmonisation minimale, à savoir que les États membres peuvent adopter ou maintenir des dispositions en vue de parvenir à un niveau de sécurité plus élevé des réseaux et des systèmes d'information que celles prévues dans la directive.

2.2 Comme elle l'a indiqué précédemment[7], la BCE soutient l'objectif de la directive NIS de garantir un niveau commun élevé de sécurité des réseaux et des systèmes d'information (NIS) 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 d'incidents de cybersécurité.

2.3 Dans un avis précédent[8], la BCE a également accueilli favorablement la nomination de la BNB en tant qu'autorité pertinente aux fins de la loi sur les infrastructures critiques, ce qui renforce la capacité de la BNB à assurer la stabilité financière et à prévenir ou atténuer les risques systémiques.

2.4 La BCE prend note de l'approche législative particulière adoptée dans le projet de loi.

D'une part, le projet de loi étend le champ d'application de la directive NIS, qui s'applique aux établissements de crédit, aux contreparties centrales et aux opérateurs de plateformes de négociation qui ont un établissement en Belgique et qui exercent effectivement en Belgique une activité liée à la fourniture d'au moins un service essentiel. En vertu du projet de loi, les infrastructures critiques notifiées par la BNB conformément à la loi sur les infrastructures critiques, sont également automatiquement considérées comme des opérateurs de services essentiels.

D'autre part, le projet de loi soumet les opérateurs de services essentiels dans le secteur financier à de simples obligations de notification d'incidents et de sanctions administratives. Toutes les autres dispositions relatives aux obligations de sécurité, aux audits interne et externe, aux contrôles, aux vérifications et aux inspections, qui s'appliquent à tous les autres secteurs ne sont pas applicables au secteur financier. Ainsi, conformément à l'article 1er, paragraphe 7, de la directive NIS, le projet de loi repose sur les compétences de surveillance prudentielle et de surveillance existantes des autorités compétentes concernées, qui imposent déjà des obligations équivalentes aux opérateurs de services essentiels pour assurer la sécurité de leurs réseaux et systèmes d'information. Les autorités concernées comprennent, au niveau européen, la BCE dans le cadre du mécanisme de surveillance unique et l'Eurosystème dans le cadre de la surveillance des infrastructures de marché. Au niveau national, les compétences de surveillance prudentielle et de surveillance existantes de la BNB sont énoncées dans la loi organique de la BNB qui confère également à la BNB des pouvoirs réglementaires, d'enquête et de sanction à l'égard de tous les établissements financiers dans l'accomplissement de ses missions. Des exigences spécifiques et

7 Voir par exemple point 2.1 de l'avis CON/2014/58, point 2.1 de l'avis CON/2017/10 et point 2.2 de l'avis CON/2018/22. Tous les avis de la BCE sont publiés sur le site internet de la BCE à l'adresse suivante : www.ecb.europa.eu.

8 Voir points 1.2 et 3.1 de l'avis CON/2014/17.

des recommandations sur la gestion du risque opérationnel sont formulées dans des législations sectorielles et des cadres applicables aux établissements de crédit[9], aux systèmes de paiement d'importance systémique[10], aux systèmes de paiement de masse considérés comme présentant une grande importance et autres systèmes de paiement de masse[11], à d'autres infrastructures des marchés financiers (y compris les contreparties centrales et les dépositaires centraux de titres[12]), aux cartes de paiement, virements, prélèvements et monnaies électroniques[13], aux prestataires de services de paiement[14], aux fournisseurs de services de réseau essentiels au sens du cadre de surveillance de l'Eurosystème[15], ainsi qu'aux processeurs d'opérations de paiement au sens de la loi belge du 24 mars 2017 sur les processeurs d'opérations de paiement[16].

2.5 En raison de cette approche législative, le projet de loi ne porte pas atteinte aux compétences actuelles de la BCE et de la BNB en ce qui concerne la surveillance prudentielle des établissements de crédit et des établissements financiers et la surveillance des infrastructures de marché. À cet égard, la BNB demeure exclusivement compétente, en vertu de ses compétences de surveillance prudentielle et de surveillance actuelles, y compris en vertu de la loi sur les infrastructures critiques, pour soumettre les opérateurs de services essentiels à des exigences de sécurité, des audits interne et externe, des contrôles, des vérifications et des inspections ainsi que d'imposer des sanctions. Les nouvelles autorités administratives créées en Belgique en vertu du projet de loi (à savoir la CCB et le DGCC) ne peuvent entraver avec ces pouvoirs de la BNB dont l'indépendance institutionnelle et opérationnelle est par conséquent garantie.

---

9 En vertu de l'article 85 de la directive (UE) 2013/36 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) les établissements de crédit mettent en œuvre des politiques et processus pour évaluer et gérer leur exposition au risque opérationnel, qui doivent également être pris en compte dans le calcul des exigences de fonds propres en vertu du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1).

10 Voir article 15 du 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), tel que modifié par le règlement (UE) 2017/2094 de la Banque centrale européenne du 3 novembre 2017 modifiant le règlement (UE) no 795/2014 concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique (BCE/2017/32) (JO L 299 du 16.11.2017, p. 11). La modification renforce davantage les obligations liées au risque opérationnel et au SRI, en tenant compte, entre autres, du document intitulé « Guidance on cyber resilience for financial market infrastructures » (Lignes directrices concernant la cyber-résilience pour les infrastructures du marché financier) du Comité des Infrastructures de Paiement et de Marché et de l'Organisation internationale des commissions de valeurs, juin 2016 (disponible en anglais sur le site internet de la BRI à l'adresse suivante : www.bis.org).

11 Voir notamment le principe 17 du document intitulé « Revised Oversight Framework for retail payment systems » (Cadre de surveillance pour les systèmes de paiement de masse révisés de l'Eurosystème), février 2016, disponible en anglais sur le site internet de la BCE.

12 Article 45 du règlement (UE) n° 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres, et modifiant les directives 98/26/CE et 2014/65/UE ainsi que le règlement (UE) n° 236/2012 (JO L 257 du 28.8.2014, p. 172) impose des exigences strictes relatives aux risques opérationnels.

13 Voir le cadre de surveillance de l'Eurosystème, juillet 2016, disponible sur le site internet de la BCE.

14 Voir articles de la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35) concernant la notification des incidents (article 96), la gestion des risques opérationnels et de sécurité (article 95) et les normes techniques de réglementation concernant l'authentification et la communication sécurisée (article 98).

15 Voir note de bas de page 13.

16 Voir article 11 de la loi du 24 mars 2017 relative à la surveillance des processeurs de transactions de paiement.

2.6 En adoptant cette approche, le projet de loi n'empiète pas sur les compétences de la BCE et de l'Eurosystème, et n'est pas contraire aux actes juridiques de l'Union existants étant donné que les obligations de notification d'incidents applicables aux opérateurs de services essentiels dans le secteur financier viennent s'ajouter au cadre de surveillance prudentielle et de surveillance existant qui continue de s'appliquer, sans ingérence indue par le projet de loi.

3. Missions de la BNB

3.1 Le projet de loi introduit dans la loi organique de la BNB un nouveau chapitre dans lequel la compétence de la BNB pour contrôler le respect par les opérateurs du secteur financier du projet de loi est formalisée. Ce nouveau chapitre, qui est inséré dans le chapitre relatif à la surveillance microprudentielle et à la surveillance macroprudentielle des établissements financiers et à la surveillance des infrastructures de marché, complète les compétences de surveillance prudentielle et de surveillance existantes de la BNB sur le secteur financier, en particulier du point de vue de la sécurité, de l'intégrité et de la résilience des réseaux et des systèmes d'information. De plus, ainsi que souligné précédemment, la BNB est l'autorité compétente en ce qui concerne la sécurité des infrastructures financières critiques[17] conformément à la loi sur les infrastructures critiques. Étant donné que le projet de loi ne confère donc pas véritablement de nouvelles missions à la BNB, la question de l'évaluation de l'attribution de nouvelles missions à une banque centrale nationale du point de vue de l'interdiction du financement monétaire ne se pose pas[18].

4. Échange d'informations avec la BCE

4.1 En vertu de l'article 9, paragraphe 1, du projet de loi, les informations concernant les opérateurs de services essentiels peuvent faire l'objet d'un échange avec des autorités de l'Union européenne, « lorsque cet échange est nécessaire à l'application de la présente loi ».

4.2 Ce libellé est trop restrictif étant donné que les informations sur les notifications d'incidents soumises par les opérateurs de services essentiels à la BNB peuvent présenter un intérêt dans d'autres contextes. Ces informations peuvent par exemple être pertinentes pour l'exercice des activités de surveillance auquel participe la BCE. Ces informations peuvent également être pertinentes dans le cadre des missions de la BCE relatives à la surveillance prudentielle des établissements de crédit en Belgique[19]. Cette surveillance prudentielle porte sur des sujets liés à la NIS dans le cadre de la surveillance prudentielle du risque opérationnel (par exemple le risque de pertes découlant d'une inadéquation ou d'une défaillance des processus, du personnel et des systèmes internes ou d'événements extérieurs, y compris le risque juridique)[20].

---

17 En ce qui concerne le rôle de la BNB en tant qu'autorité compétente pour la sécurité et la protection des infrastructures critiques, voir avis CON/2014/17, points 3.1 et 3.5.

18 Voir point 2.3 de l'avis CON/2018/15.

19 Voir règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit (JO L 287 du 29.10.2013, p. 63).

20 Voir point 4.3 de l'avis CON/2018/22.

Dans ce contexte, la BCE recommande d'améliorer le libellé de l'article 9 du projet de loi pour garantir que la BNB partage ces informations avec la BCE en temps utile et avec efficacité, dans le cadre des responsabilités de la BCE en ce qui concerne la surveillance des systèmes de paiement et la surveillance prudentielle des établissements de crédit[21].

Cet avis sera publié sur le site internet de la BCE.

Fait à Francfort-sur-le-Main, le 18 mai 2018.

[signé]

Le président de la BCE

Mario DRAGHI

21 Voir point 6.2 de l'avis CON/2018/22.