PARECER DO BANCO CENTRAL EUROPEU

de 11 de abril de 2022

sobre uma proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Introdução e base jurídica

Em 16 de dezembro de 2020, a Comissão Europeia adotou uma proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 ([1]) (a seguir «diretiva proposta»). Em 3 de dezembro de 2021, o Conselho da União Europeia definiu a sua orientação geral sobre a diretiva proposta ([2]). A competência do Banco Central Europeu (BCE) para emitir parecer baseia-se no artigo 127.º, n.º 4, segundo parágrafo, do Tratado sobre o Funcionamento da União Europeia, uma vez que a diretiva proposta contêm disposições que se inserem nas competências do BCE, nomeadamente nas de promoção do bom funcionamento dos sistemas de pagamentos e de contribuição para a boa condução das políticas prosseguidas pelas autoridades competentes relativas à estabilidade do sistema financeiro, bem como nas atribuições do BCE relativas à supervisão prudencial das instituições de crédito nos termos do artigo 127.º, n.º 2, quarto travessão, do artigo 127.º, n.º 5, e do artigo 127.º, n.º 6, do Tratado. O presente parecer foi aprovado pelo Conselho do BCE nos termos do artigo 17.º-5, primeiro período, do Regulamento Interno do Banco Central Europeu.

Observações genéricas

O BCE apoia firmemente os objetivos da diretiva proposta de aumentar o nível de ciber-resiliência em todos os setores relevantes, reduzir as incoerências no mercado interno e aumentar o nível de conhecimento da situação e a capacidade coletiva de preparação e resposta, assegurando uma cooperação eficiente na União.

O BCE reconhece a importância de manter ligações fortes entre a diretiva proposta e o setor financeiro, que deve continuar a fazer parte do ecossistema de redes e da informação (SRI), a fim de promover uma avaliação coerente dos riscos relacionados com as tecnologias da informação e comunicação (TIC) em toda a União e um intercâmbio de informações e uma colaboração intersectoriais eficazes na gestão das ciberameaças. Para este efeito, deverá ser possível às autoridades competentes nos termos da proposta de regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro ([3]) (a seguir «Regulamento DORA») participar nos debates políticos estratégicos e no funcionamento técnico do Grupo de Cooperação SRI, bem como trocar informações e continuar a cooperar com os pontos de contacto únicos e as equipas nacionais de resposta a incidentes de segurança informática referidos na diretiva proposta ([4]).

1. Finalidade da diretiva proposta

1.1 O BCE entende que, relativamente e às entidades do setor financeiro, o Regulamento DORA será considerado como legislação setorial específica que introduz exigências em matéria de gestão dos riscos de cibersegurança e de notificação de incidentes cujos efeitos são, pelo menos, equivalentes aos das exigências estabelecidas na diretiva proposta ([5]). Por conseguinte, as disposições da diretiva proposta em matéria de obrigações de gestão dos riscos de cibersegurança e de notificação, partilha de informações, supervisão e execução coerciva não serão aplicáveis a quaisquer entidades financeiras abrangidas pelo Regulamento DORA ([6]). Tal como clarificado nos considerandos da

([1]) COM(2020) 823 final.
([2]) Disponível no sítio *web* do Conselho em www.consilium.europa.eu
([3]) COM(2020) 595 final.
([4]) Ver o ponto 1.5 do Parecer CON/2021/20 do Banco Central Europeu, de 4 de junho de 2021, sobre uma proposta de regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro (JO C 343 de 26.8.2021, p. 1). Todos os pareceres do BCE estão publicados no EUR-Lex. Artigos 17.º, n.º 5, e 42.º do Regulamento DORA; artigo 11.º da diretiva proposta.
([5]) Artigo 2.º, n.º 6 da diretiva proposta.
([6]) Considerando 13 e artigo 2.º, n.º 6, da diretiva proposta.

diretiva proposta, em lugar das disposições estabelecidas na diretiva proposta, devem aplicar-se as disposições do Regulamento DORA relativas às medidas de gestão dos riscos no domínio das TIC, à gestão de incidentes relacionados com TIC e, em especial, à notificação de incidentes, bem como as relativas a testes de resiliência operacional digital, acordos de partilha de informações e riscos de terceiros no domínio das TIC, devem ser aplicadas ([7]).

1.2 O BCE observa também que o Conselho, na sua orientação geral sobre a diretiva proposta, apresenta uma alteração destinada a excluir da aplicação da diretiva proposta as «entidades que exercem atividades nos domínios do poder judicial, dos parlamentos ou dos bancos centrais» ([8]). O BCE entende que a alteração proposta seria extensiva a todas as atribuições e competências fundamentais do Sistema Europeu de Bancos Centrais (SEBC) estabelecidas no artigo 127.º, n.º 2, do Tratado e no artigo 3.º-1 dos Estatutos do Sistema Europeu de Bancos Centrais e do Banco Central Europeu (a seguir «Estatutos do SEBC»), nomeadamente a promoção do bom funcionamento dos sistemas de pagamentos. A este respeito, considera-se que as infraestruturas dos mercados financeiros detidas e operadas pelo Eurosistema, tais como o TARGET2 e o TARGET2-Securities, são abrangidas pela proposta pelo Conselho de excluir os bancos centrais do âmbito de aplicação da diretiva proposta.

2. **Competências de fiscalização do SEBC e do Eurosistema**

2.1 Paralelamente ao objetivo primordial do SEBC de manutenção da estabilidade de preços, e em conformidade com o artigo 127.º, n.º 2, do Tratado, uma das atribuições fundamentais cometidas ao SEBC consiste na promoção do bom funcionamento dos sistemas de pagamentos ([9]). No desempenho desta atribuição, «[O] BCE e os bancos centrais nacionais podem conceder facilidades e o BCE pode adotar regulamentos, a fim de assegurar a eficiência e a solidez dos sistemas de compensação e de pagamentos no interior da União e com países terceiros» ([10]). No exercício da sua função de superintendência, o BCE adotou o Regulamento do Banco Central Europeu (UE) n.º 795/2014 (BCE/2014/28) ([11]) (a seguir «Regulamento SIPS»), que transpõe os Princípios para as Infraestruturas dos Mercados Financeiros estabelecidos pelo CPSS e pela IOSCO ([12]) para legislação diretamente aplicável. O Regulamento SIPS estabelece requisitos tanto para sistemas de pagamentos de grande montante como de retalho de importância sistémica, sejam de titularidade pública ou privada. Os requisitos previstos no Regulamento SIPS já incluem, entre outros, a gestão dos riscos operacionais e a instituição de um quadro de ciber-resiliência ([13]).

2.2 Para além dos sistemas de pagamentos sistemicamente importantes, a superintendência do Eurosistema abrange os sistemas de pagamentos de importância não sistémica, os instrumentos, esquemas e acordos de pagamento eletrónico, bem como outras infraestruturas e prestadores de serviços críticos, tal como estabelecido no quadro da política de superintendência do Eurosistema ([14]). Os sistemas de pagamentos e os demais mecanismos sujeitos à superintendência do Eurosistema não estão expressamente incluídos no âmbito de aplicação da diretiva proposta ([15]). Ao mesmo tempo, dado que a diretiva proposta é um instrumento de harmonização mínima ([16]), a legislação de execução adotada pelos Estados-Membros poderia acabar por sobrepor-se às competências do Eurosistema em matéria de superintendência. Para evitar tal situação, as competências do SEBC previstas no Tratado e nos Estatutos do SEBC, bem como as competências do Eurosistema previstas no Regulamento SIPS e, de um modo geral, no Quadro da Política de Superintendência do Eurosistema, deveriam ser expressamente reconhecidas nos considerandos da diretiva proposta.

([7]) Considerando 13 da diretiva proposta.
([8]) Artigo 2.º, n.º 3-A, primeiro parágrafo, alínea b), da orientação geral do Conselho sobre a diretiva proposta.
([9]) Artigo 127.º, n.º 2, do TFUE, tal como refletido no artigo 3.º-1 dos Estatutos do SEBC.
([10]) Artigo 22.º dos Estatutos do SEBC.
([11]) Regulamento (UE) n.º 795/2014 do Banco Central Europeu, de 3 de julho de 2014, relativo aos requisitos de superintendência de sistemas de pagamentos sistemicamente importantes (BCE/2014/28) (JO L 217 de 23.7.2014, p. 16).
([12]) Ver Comité dos Sistemas de Pagamentos e Liquidação (Committee on Payment and Settlement Systems – CPSS), do Banco de Pagamentos Internacionais, e Comité Técnico da Organização Internacional das Comissões de Valores Mobiliários (International Organization of Securities Commissions – IOSCO), Principles for Financial Market Infrastructures (Princípios para as Infraestruturas dos Mercados Financeiros), abril de 2012, disponíveis no sítio *Web* do Banco de Pagamentos Internacionais em www.bis.org. A responsabilidade D estabelece que «se espera que todos os membros do CPSS e da IOSCO apliquem os princípios às pertinentes infraestruturas dos mercados financeiros das respetivas jurisdições na medida do permitido pelos quadros jurídicos nacionais».
([13]) Artigo 15.º do Regulamento (UE) n.º 795/2014 (BCE/2014/28).
([14]) *Eurosystem overoversight policy framework* (Quadro da política de superintendência do Eurosistema), versão revista (julho de 2016) disponível [*em inglês*] no sítio *Web* do BCE em www.ecb.europa.eu.
([15]) Artigo 2.º da diretiva proposta e anexos I e II da diretiva proposta.
([16]) Artigo 3.º da diretiva proposta.

3. **Risco de terceiros no domínio das TIC, gestão de incidentes e crises em grande escala, partilha de informações e estratégia nacional de cibersegurança**

3.1 *Gestão de riscos de terceiros no domínio das TIC*

3.1.1 A diretiva proposta habilita as autoridades competentes, no exercício dos seus poderes de execução coerciva em relação a entidades essenciais, a emitir instruções vinculativas ou uma ordem que exija que essas entidades corrijam as deficiências detetadas ou as infrações às obrigações previstas na diretiva proposta ([17]). Ao mesmo tempo, a «Autoridade Fiscalizadora Principal» designada nos termos do Regulamento DORA pode formular recomendações a entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas para que assegurem a gestão dos potenciais riscos sistémicos decorrentes das práticas de subcontratação e de concentração de serviços de TIC prestados por terceiros ([18]).

3.1.2 Considerando que uma «entidade essencial» nos termos da diretiva proposta pode também ser designada como «entidade terceira prestadora de serviços no domínio das TIC considerada crítica» nos termos do DORA, o BCE reitera ([19]) que deveria ser evitada a formulação de recomendações contraditórias e de instruções vinculativas. A este respeito, o BCE congratula-se com a orientação geral do Conselho sobre a diretiva proposta. De acordo com esta abordagem, as autoridades competentes devem informar o «Fórum de Fiscalização», instituído ao abrigo do Regulamento DORA, quando exercem os seus poderes de supervisão e de execução coerciva em relação a uma entidade essencial designada como entidade terceira prestadora de serviços no domínio das TIC considerada crítica nos termos do Regulamento DORA ([20]).

3.2 *Gestão de incidentes e crises em grande escala*

3.2.1 Em conformidade com a diretiva proposta ([21]), os Estados-Membros devem designar uma ou mais autoridades competentes responsáveis pela gestão de incidentes e crises em grande escala. Como se esclarece nos considerandos da diretiva proposta, entende-se por incidente em larga escala um incidente com um impacto significativo em, pelo menos, dois Estados-Membros ou que cause perturbações tão extensas que ultrapassem a capacidade de resposta de um Estado-Membro. Os incidentes em grande escala podem transformar-se em verdadeiras crises que impedem o correto funcionamento do mercado interno ([22]).

3.2.2 Embora as autoridades competentes designadas ao abrigo do Regulamento DORA permaneçam responsáveis pela gestão dos incidentes de cibersegurança respeitantes a entidades financeiras, a cooperação com as estruturas e autoridades instituídas nos termos da diretiva proposta será fundamental para assegurar uma resposta coordenada em toda a União. Para este efeito, o BCE acolheria favoravelmente a participação das autoridades competentes designadas ao abrigo do Regulamento DORA, incluindo o BCE, na Rede Europeia de Organizações de Coordenação de Cibercrises (EU-CyCLONe) ([23]), sempre que incidentes e crises de cibersegurança em grande escala afetem o setor financeiro.

3.3 *Partilha de informações*

3.3.1 Tal como acima referido, o BCE apoia firmemente a cooperação entre as autoridades competentes designadas ao abrigo do Regulamento DORA e as estruturas e autoridades instituídas nos termos da diretiva proposta. A partilha de informações entre as autoridades pode, nomeadamente, permitir a aprendizagem intersectorial, contribuir para a prevenção e a gestão eficaz de ciberataques e promover uma avaliação coerente dos riscos relacionados com as TIC em toda a União. O BCE salienta, no entanto, que o intercâmbio de informações deve ter lugar apenas quando existam mecanismos de classificação e de partilha de informações claramente definidos, juntamente com salvaguardas adequadas para garantir a confidencialidade ([24]). O BCE congratula-se com a orientação geral do

([17]) Artigo 29.º, n.º 4, alínea b), da diretiva proposta.
([18]) Artigo 31.º do Regulamento DORA.
([19]) Ver o ponto 1.2 do Parecer CON/2021/20.
([20]) Artigo 29.º, n.º 10, da orientação geral do Conselho sobre a diretiva proposta.
([21]) Artigo 7.º, n.º 1, da diretiva proposta.
([22]) Considerando 27 da diretiva proposta.
([23]) Artigo 14.º da diretiva proposta.
([24]) Ver o ponto 1.5 do Parecer CON/2021/20.

Conselho sobre diretiva proposta, que preconiza o intercâmbio regular de informações relevantes entre as autoridades ([25]), o estabelecimento de acordos de cooperação que especifiquem um mecanismo de intercâmbio de informações ([26]) e a transmissão automática e direta das notificações de incidentes ([27]). Nesta conformidade, importa assegurar que as informações confidenciais previstas nas disposições relativas ao sigilo profissional do Regulamento DORA ([28]) ou da legislação setorial pertinente ([29]) só possam ser permutadas com as autoridades competentes referidas na proposta de diretiva se esse intercâmbio for necessário à aplicação das disposições da diretiva proposta pelas autoridades competentes ([30]).

3.4 *Estratégia nacional de cibersegurança*

3.4.1 Nos termos da diretiva proposta, os Estados-Membros devem adotar uma estratégia nacional de cibersegurança que defina objetivos estratégicos e medidas políticas e regulamentares adequadas, com vista a alcançar e manter um elevado nível de cibersegurança ([31]). Como se esclarece nos considerandos da diretiva proposta, os Estados-Membros devem continuar a incluir o setor financeiro nas respetivas estratégias de cibersegurança ([32]). A título indicativo, no âmbito das suas estratégias nacionais de cibersegurança, os Estados-Membros deveriam adotar políticas relativas à cibersegurança na cadeia de abastecimento dos produtos e serviços de TIC utilizados pelas diferentes entidades para a prestação dos respetivos serviços. No que se refere ao setor financeiro, as estratégias nacionais de cibersegurança devem ser coerentes com o quadro normativo decorrente do Regulamento DORA. A este respeito, o BCE considera que são necessários esclarecimentos complementares para assegurar que as estratégias nacionais de cibersegurança são coerentes com a legislação setorial específica.

Nos casos em que o BCE recomenda alterações à diretiva proposta, as sugestões de reformulação específicas constam de um documento técnico de trabalho separado, acompanhadas de um texto explicativo para o efeito. O documento técnico de trabalho está disponível em inglês no EUR-Lex.

Feito em Frankfurt am Main, em 11 de abril de 2022.

A Presidente do BCE
Christine LAGARDE

([25]) Artigo 11.º, n.º 5, da orientação geral do Conselho sobre a diretiva proposta.
([26]) Considerando 23-A da orientação geral do Conselho sobre a diretiva proposta.
([27]) Considerando 13 da orientação geral do Conselho sobre a diretiva proposta.
([28]) Artigo 49.º do Regulamento DORA.
([29]) Artigos 53.º a 62.º da Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).
([30]) Artigos 2.º, n.º 5, e 11.º, n.º 4, da diretiva proposta.
([31]) Artigo 5.º da diretiva proposta.
([32]) Considerando 13 da diretiva proposta.