Comentários da Associação Portuguesa de Bancos à consulta pública relativa à Proposta de Lei de autorização legislativa para aprovação do novo Regime Jurídico da Cibersegurança, transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, destinada a garantir um elevado nível comum de cibersegurança em toda a União Europeia (NIS2)

A. Enquadramento

O Gabinete do Ministro da Presidência submeteu a consulta pública, no passado dia 21 de novembro de 2024, com prazo de resposta até ao dia 12 de dezembro de 2024, a Proposta de Lei de autorização legislativa e respetivo Decreto-Lei autorizado, para aprovação do novo Regime Jurídico da Cibersegurança, transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, destinada a garantir um elevado nível comum de cibersegurança em toda a União Europeia (NIS2).

A Associação Portuguesa de Bancos, enquanto entidade que representa o sector bancário, considerado, no âmbito de aplicação da NIS2, como um sector de importância crítica, pronuncia-se relativamente a esta consulta pública, apresentando os contributos recebidos dos seus Associados.

B. A necessidade de adequada articulação entre o Regulamento DORA e o diploma nacional de transposição da Diretiva NIS2 e de não duplicação dos requisitos a que ficam sujeitos os bancos nacionais

A Diretiva (UE) n.º 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro (Diretiva NIS2) relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que altera o Regulamento (UE) n. 910/2014 e a Diretiva (UE) 2018/1972, e revoga a sua antecessora, a Diretiva (UE) 2016/1148 (Diretiva NIS1), tem como objetivo central eliminar as divergências verificadas no contexto da aplicação da Diretiva NIS1 entre os Estados-Membros, visando assim uma maior harmonização através do estabelecimento de regras mínimas relativas ao funcionamento de um quadro regulamentar coordenado.

Esta Diretiva NIS2 estabelece um quadro comum no domínio da cibersegurança, sujeito a transposição para o direito nacional, e que inclui nomeadamente (i) exigências, dirigidas aos Estados-Membros, que devem garantir um elevado nível de cibersegurança e reforçar a cooperação entre as autoridades competentes pela cibersegurança; (ii) medidas de gestão dos riscos de cibersegurança e de notificação de informações em sectores críticos, sujeitando os principais operadores dos sectores-chave a adotarem as medidas de segurança necessárias e notificarem as autoridades competentes de qualquer incidente com impacto significativo na prestação dos seus serviços; (iii) regras relativas à partilha de informações; e, ainda (iv) disposições sobre a supervisão e o *enforcement* ("execução") deste quadro.

Por sua vez, o Regulamento (UE) n.º 2022/2554, do Parlamento Europeu e do Conselho, de 14 de dezembro (Regulamento DORA), visa reforçar a resiliência operacional das instituições financeiras na União Europeia, nomeadamente através da gestão de riscos sistémicos, do reforço da resiliência digital e da introdução de normas relativas a testes de penetração regulares e comunicação de incidentes, com o objetivo de assegurar a cibersegurança e a resiliência das redes e dos serviços que suportam a atividade das entidades do sector financeiro na União Europeia, entrando em vigor a partir do próximo dia 17 de janeiro de 2025.

As instituições de crédito estão abrangidas no âmbito de aplicação do Regulamento DORA, que é de aplicação direta nos Estados-Membros, e, no caso das instituições de crédito consideradas entidades essenciais ou importantes, nos termos das regras nacionais de transposição da Diretiva NIS2, estas ficam igualmente abrangidas no âmbito de aplicação desta diretiva e respetivo diploma nacional de transposição.

Contudo, o Regulamento DORA é expressamente considerado um "ato jurídico sectorial da União", para efeitos da Diretiva NIS2, aí se prevendo (Considerando 28) que "*O Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho deverá ser considerado um ato jurídico sectorial da União para efeitos da presente diretiva no que diz respeito às entidades financeiras.*".

Daí decorre um estatuto de equivalência entre as disposições da NIS2 e do Regulamento DORA, expressamente reconhecido em ambos os textos legais europeus, e na Comunicação da Comissão Europeia (2023/C 328/02), relativa às Orientações da Comissão sobre a aplicação do Artigo 4.º, n.ºs 1 e 2, da Diretiva NIS2), assim como a não aplicabilidade de um conjunto de disposições da NIS2 às entidades obrigadas no âmbito do Regulamento DORA (nosso negrito e sublinhado):

- **Diretiva NIS2** –

  Considerando (28) *"(…)**. As disposições do Regulamento (UE) 2022/2554 relativas às medidas de gestão dos riscos no domínio das tecnologias da informação e comunicação (TIC), à gestão de incidentes relacionados com TIC e, em especial, às obrigações de notificação de incidentes de caráter severo relacionados com as TIC, bem como as relativas a testes de resiliência operacional digital, acordos de partilha de informações e riscos de terceiros no domínio das TIC, deverão ser aplicadas em vez das disposições previstas na presente diretiva.* **Por conseguinte, os Estados-Membros não deverão aplicar as disposições da presente diretiva em matéria de obrigações de gestão dos riscos de cibersegurança e de notificação, e em matéria de supervisão e execução, relativas às entidades financeiras abrangidas pelo Regulamento (UE) 2022/2554** *(..)"*

  Artigo 4.º -Atos jurídicos sectoriais da União – n.º 1. *"**Sempre que atos jurídicos sectoriais da União exijam que entidades essenciais e importantes adotem medidas de gestão dos riscos de cibersegurança ou notifiquem incidentes significativos, e se tais requisitos forem, na prática, pelo menos equivalentes às***

obrigações estabelecidas na presente diretiva, não se aplicam a essas entidades as disposições pertinentes da presente diretiva, nomeadamente as disposições em matéria de supervisão e execução estabelecidas no capítulo VII *(…).”*

- **Regulamento DORA** –

  Artigo 1.º n.º 2 – *“Quanto às entidades financeiras identificadas como entidades essenciais ou importantes nos termos das regras nacionais que transpõem o artigo 3.º da Diretiva (UE) 2022/2555,* ***considera-se que o presente regulamento constitui um ato jurídico sectorial da União para efeitos do artigo 4.º da referida diretiva****.”*

- **Comunicação C/2023/6068** –

  Apêndice - Atos jurídicos sectoriais da União: *“Regulamento (UE) 2022/2554 (Regulamento Resiliência Operacional Digital)*

  1. …. Consequentemente, as disposições do Regulamento (UE) 2022/2554 relativas à gestão do risco associado às tecnologias da informação e comunicação (TIC) (artigo 6.º e seguintes), à gestão de incidentes relacionados com as TIC e, em especial, às obrigações de notificação de incidentes de caráter severo relacionados com as TIC (artigo 17.º e seguintes), bem como as relativas a testes de resiliência operacional digital (artigo 24.º e seguintes), acordos de partilha de informações (artigo 25.º) e risco associado às TIC devido a terceiros (artigo 28.º e seguintes) são aplicáveis em vez das disposições previstas na Diretiva (UE) 2022/2555. ***Por conseguinte, os Estados-Membros não devem aplicar as disposições da Diretiva (UE) 2022/2555 em matéria de obrigações de gestão dos riscos de cibersegurança e de notificação, e em matéria de supervisão e execução, às entidades financeiras abrangidas pelo Regulamento (UE) 2022/2554.***

  2. Neste contexto, consideram-se entidades financeiras as entidades a que se refere o artigo 2.º, n.º 1, alíneas a) a t), do Regulamento (UE) 2022/2554. ***Os tipos de entidades abrangidas pelo âmbito de aplicação do Regulamento (UE) 2022/2554 enquanto entidades financeiras, bem como pelo âmbito de aplicação da Diretiva (UE) 2022/2555 enquanto entidades essenciais ou importantes, incluem instituições de crédito****…”*

Cumpre salientar também que o Centro Nacional de Cibersegurança (CNCS), no seu sítio da *internet*, na área de supervisão e regulação, apresenta um conjunto de perguntas frequentes relativas à Diretiva NIS2, no qual aborda a questão “*Como se articula a Diretiva SRI2 com o Regulamento DORA, aplicável ao sector financeiro?*”, reforçando os pontos acima descritos.

No entanto, na Proposta de Lei, respetivo Decreto-Lei autorizado e Regime Jurídico da Cibersegurança anexo, agora submetidos a consulta pública, a única referência relativa à notificação de incidentes no sector financeiro, surge no n.º 1 do Artigo 59.º (Comunicação de incidentes e aplicação de medidas), no qual se refere que "*As autoridades nacionais sectoriais de cibersegurança e as autoridades nacionais especiais de cibersegurança informam o CNCS da ocorrência de incidentes ou ciberameaças significativas, bem como da aplicação de medidas de supervisão e de execução, nos termos do artigo 53.º e seguintes.*"

Conforme estabelece a alínea b), do número 2, do Artigo 15º do referido Regime Jurídico da Cibersegurança, as autoridades nacionais especiais de cibersegurança, no que respeita à matéria da resiliência operacional digital do sector financeiro, são a Autoridade de Seguros e Pensões (ASF), a Comissão do Mercado de Valores Mobiliários (CMVM) e o Banco de Portugal.

Por conseguinte, não resulta claro, no regime de transposição da NIS2 consagrado na Proposta de Lei em apreço, que o sector bancário não ficará, de acordo com a presente proposta de transposição, sujeito a uma "duplicação" de requisitos exigidos (por exemplo, quanto à notificação obrigatória de incidentes, quer ao Banco de Portugal, quer ao CNCS), situação que, contudo, sempre contrariaria o espírito e a letra da legislação europeia que se pretende transpor.

Assim, **considera-se fundamental que a transposição desta Diretiva para o enquadramento legal nacional (i) seja esclarecedora e inequívoca relativamente à não aplicabilidade de um conjunto de disposições da NIS2 às entidades obrigadas ao DORA** (e.g. disposições em matéria de obrigações de gestão dos riscos de cibersegurança e de notificação, e em matéria de supervisão e execução), **e (ii) que evite a duplicação de requisitos de notificação e de metodologias diferenciadas, atendendo ao enquadramento legal europeu que, para o sector financeiro, preconiza claramente a harmonização/uniformização dos requisitos em matéria de ciberresiliência**.

De outra forma, as Instituições de Crédito nacionais ficariam sujeitas a um quadro mais gravoso e divergente do que aquele a que ficarão sujeitas as suas congéneres europeias, com custos e deveres acrescidos, sem que daí resultasse quaisquer benefícios para o cumprimento dos objetivos das medidas legislativas em apreço.

Em face do supra exposto, mostra-se, assim, necessário consagrar uma disposição adicional, no Regime Jurídico da Cibersegurança, segundo a qual se estabeleça:

"Às entidades financeiras abrangidas pelo âmbito de aplicação do Regulamento (UE) 2022/2554 (Regulamento Resiliência Operacional Digital), considerado um ato jurídico sectorial da União Europeia, para efeitos do artigo 4.º da Diretiva (UE) 2022/2555, não serão aplicáveis as disposições do presente regime, em

***matéria de obrigações de gestão dos riscos de cibersegurança e de notificação (Capítulos IV e V), e em matéria de supervisão e execução (Capítulo VI), aplicando-se, ao invés, o regime estabelecido nesse Regulamento.*"**

C. Reforço do quadro de combate às fraudes com recurso a redes de comunicações e plataformas digitais

O sector bancário está empenhado em fazer a sua parte no combate às práticas fraudulentas associadas à usurpação de números de telefone ou identificadores de mensagens, nomeadamente campanhas de *smishing* e *vishing* com *spoofing* realizadas em Portugal, que atingem, de forma transversal, todos os sectores da sociedade, conhecendo-se casos, em Portugal, de ataques realizados através da usurpação da identidade de diversas entidades públicas e privadas.

De entre as soluções mais essenciais e eficazes de combate a esta criminalidade, destacamos as que envolvem a aplicação de medidas técnicas, operacionais e organizativas, por parte dos operadores responsáveis pelas redes de comunicações, assim como pelas plataformas digitais. Nesse sentido no âmbito do novo Regime da Cibersegurança em apreço considera-se imprescindível que se preveja expressamente um enquadramento claro e adequado quanto à adoção dessas medidas.

O reforço do quadro legal, e a inclusão de mecanismos de combate à fraude na proposta legislativa em apreço afigura-se particularmente relevante encontrando suporte, não só na necessidade de o legislador nacional atuar, de forma tempestiva, para evitar uma progressão das ameaças em causa, como também no facto de a Diretiva NIS2 abordar precisamente estas matérias, designadamente, prevendo, no respetivo artigo 21.º n.º 1 que "*as entidades essenciais e importantes tomam medidas técnicas, operacionais e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança dos sistemas de rede e informação que utilizam nas suas operações ou na prestação dos seus serviços e para impedir ou minimizar o impacto de incidentes nos destinatários dos seus serviços e noutros serviços*".

Por conseguinte, na linha das medidas já adotadas ou em adoção em diversos outros Estados-Membros da UE - a título meramente exemplificativo, referimos os casos da Finlândia (chamadas e SMS), França ou Espanha -, propõe-se a inclusão de uma disposição adicional (nomeadamente no artigo 57.º do novo Regime da Cibersegurança), que preveja a obrigação dos prestadores de serviços e redes de comunicações eletrónicas, de plataformas de mercados em linha ou de redes sociais, adotarem todas as medidas técnicas, operacionais e organizativas necessárias a prevenir que os seus sistemas de redes e informação, e os serviços por si prestados, sejam utilizadas em atividades fraudulentas. Tais medidas deverão incluir pelo menos, as seguintes disposições:

(a) Confirmação da autenticidade e legitimidade de todas as chamadas e mensagens encaminhadas através das redes de telecomunicações, tomando as ações necessárias para impedir a utilização de um determinado número

para finalidades relacionadas com fraude, nomeadamente através do bloqueio do chamador ou do remetente da mensagem com identificador usurpado.

(b) Disponibilização da possibilidade de registo de identificação de remetentes de SMS, que deverá ser utilizado como referencial de validação de autenticidade/legitimidade para futuros envios, impedindo qualquer tentativa de utilização que não se enquadre nos padrões desse registo. Tal registo de identificação de remetentes de SMS deverá ser necessariamente precedido de um processo de verificação da autenticidade e legitimidade da entidade que o solicita (ou do respetivo representante), bem como da sua autorização para esse efeito.

(c) Prevenção da criação de sítios na internet que sejam utilizados para fins fraudulentos e obstaculização a que os motores de pesquisa da Internet exibam esses sítios na internet na lista de resultados de pesquisa, nomeadamente no perímetro de actuação e comunicações passíveis de controlo ou intervenção por cada operador.

(d) Adoção mandatória de medidas de verificação de identidade e de diligência devida, relativamente aos seus clientes.

D. Outros comentários específicos

Artigo 6º do Decreto-Lei autorizado - Norma revogatória

No Decreto-Lei autorizado anexo à Proposta de Lei, é referido que são revogados o Regime Jurídico da Segurança do Ciberespaço, aprovado pela Lei n.º 46/2018, de 13 de agosto e a Regulamentação do Regime Jurídico da Segurança do Ciberespaço, aprovada pelo Decreto-Lei n.º 65/2021, de 30 de julho (alíneas b e c).

No entanto, não é claro se o Regulamento n.º 183/2022, de 21 de fevereiro de 2022, regulamento que configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança (Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes), que faz parte do atual Regime Jurídico da Segurança do Ciberespaço, também é revogado.

De notar que, no Artigo 41.º, n.º 4, é referido que "O formato e procedimento de notificação de incidentes e a taxonomia dos incidentes, incluindo as categorias de causas dos incidentes e os seus efeitos, são definidos por instrução técnica do CNCS, sem prejuízo dos atos de execução adotados pela Comissão previstos no n.º 11 do artigo 23.º da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro.", não sendo claro se será uma nova instrução técnica ou a já existente no Regulamento n.º 183/2022.

Regime Jurídico da Cibersegurança - Artigo 40.º Notificação obrigatória

Conforme já anteriormente sublinhado, é importante que a transposição da Diretiva NIS2 para a legislação nacional seja esclarecedora e inequívoca relativamente à não aplicabilidade ao sector bancário das disposições, em particular, as referentes às obrigações de notificação, de forma a evitar a duplicação de requisitos de notificação e metodologias diferenciadas.

* * *