ANTAS
DA CUNHA
ECIJA

REVISÃO DO REGULAMENTO CIBERSEGURANÇA DA UNIÃO EUROPEIA:

UMA PROPOSTA CONTROVERSA E DEBATIDA

Artigo da autoria de:

José Luís da Cruz Vilaça

Paulo de Almeida Sande

Mariana Tavares

Ecija 2026

Introdução e contexto

Em 20 de janeiro de 2026, a Comissão Europeia ("**CE**") publicou um pacote legislativo que inclui a substituição do Regulamento da Cibersegurança da União Europeia ("**CSA"**).[1]

O pacote altera a NIS2[2] e está interligado com a CSA, ao mesmo tempo que cumpre outras leis e regulamentos relacionados com o Pacote Omnibus Digital. [3]

Este artigo centra-se na proposta para substituir a CSA. Esta entrou em vigor em 2019, desenvolvendo o papel da ENISA[4] e estabelecendo um quadro voluntário para a certificação da segurança das tecnologias da informação e das comunicações ("**TIC**"). Substituiu os "regimes nacionais fragmentados" e garantiu a segurança dos produtos, serviços e processos a diferentes níveis, estabelecendo os regimes do Quadro Europeu de Certificação da Cibersegurança ("**ECCF**"). Incluiu a segurança da Internet das Coisas, entre outros questões relacionadas com cibersegurança.

A revisão da CSA, apresentada em janeiro de 2026 ("**CSA2**" ou "**a proposta**"), tem dois objetivos principais: (i) aumentar as capacidades e a resiliência em matéria de cibersegurança e (ii) evitar a fragmentação no mercado único.

São consideradas quatro áreas de intervenção: (i) reforço do mandato da ENISA, (ii) reforma do ECCF, (iii) simplificação dos procedimentos, principalmente através de alterações específicas à

NIS2 interligadas com a CSA, e (iv) segurança das cadeias de abastecimento das TIC.

Entre outras disposições, a CS2 exige a eliminação progressiva obrigatória dos componentes TIC nas redes 5G enumerados no anexo II,[5] fornecidos por fornecedores de alto risco - *high-risk suppliers* ("**HRS**").[6]

No chamado "5G security toolbox" (referido pela ANACOM e pela CE como "conjunto de instrumentos da UE para a segurança das redes 5G"), aprovado pela CE em 29 de janeiro de 2020 e de natureza não vinculativa, recomendava-se a restrição da utilização de equipamentos 5G de fornecedores de alto risco.

Se o pacote de políticas que a CE diz preferir for adotado, esta recomendação tornar-se-á obrigatória.

A proposta estabelece também um Quadro Europeu de Certificação da Cibersegurança («**ECCF**») simplificado, alargando o seu âmbito para incluir fatores mais amplos, tais como forças geopolíticas e a ameaça representada pelas tecnologias emergentes, incluindo a IA e a criptoanálise quântica.

A proposta foca os HRS no seu novo quadro, supostamente para garantir a segurança das cadeias de abastecimento de TIC de entidades que operam em setores altamente críticos, tal como definido pela NIS2. Caracteriza os HRS — conceito mencionado 63 vezes na proposta — como suscetíveis à influência de um governo não pertencente ao Espaço Económico Europeu de uma forma que poderia comprometer a

continuidade do serviço e a segurança dos dados ou afetar a integridade dos produtos ou serviços fornecidos.

Para além de designar os HRS, a CE pretende também identificar países terceiros que suscitam preocupações em matéria de cibersegurança. A partir daí, são visadas entidades estabelecidas ou controladas por um país terceiro que apresenta riscos de cibersegurança, entidades estabelecidas nesse país ou um dos seus nacionais. A CE reconhece que os incidentes significativos de cibersegurança na cadeia de abastecimento se propagam frequentemente além das fronteiras nacionais.[7] Na proposta do futuro Quadro Financeiro Plurianual 2028-2034, há mesmo uma previsão de exclusão dos HRS como princípio estruturante, a fim de proteger a integridade do orçamento da UE e os interesses de segurança.

De acordo com a CE, o objetivo deste novo regulamento é criar um quadro harmonizado para combater «os riscos não técnicos que afetam as cadeias de abastecimento das TIC»,[8] a fim de reduzir «a atual fragmentação das abordagens entre os Estados-Membros». [9] A CE afirma que a proposta representa «uma simplificação e modernização substanciais do quadro jurídico da União em matéria de cibersegurança, em plena conformidade com os princípios REFIT[10] de clareza, eficiência e preparação digital»[11].

No seu relatório de avaliação de impacto sobre a proposta (*Impact Assessment Report*), a CE enumera as várias opções possíveis para as quatro áreas de intervenção acima mencionadas, que recordamos: o

mandato da ENISA, o ECCF, a simplificação através de alterações à NIS2 e a segurança da cadeia de abastecimento das TIC.

Estas opções são apresentadas como o resultado de uma análise exaustiva para determinar o nível e a forma de intervenção mais adequados, incluindo se a ação da UE conduziria a melhores resultados do que as soluções dos Estados-Membros isoladamente. [12]

É importante salientar que a análise da CE concluiu que a ação da UE conduziria a melhores resultados do que a ação isolada dos Estados-Membros, mas isso não permite a violação dos princípios fundamentais do direito da União, em particular no que diz respeito à repartição de competências.

Sobre as diferentes opções apresentadas para cada uma das quatro áreas de intervenção, a CE indica o "pacote de políticas" que prefere:[13]

- A reforma funcional da ENISA;

- A reforma do ECCF, incluindo um alargamento do seu âmbito de aplicação, um novo procedimento e uma governação revista;

- Uma intervenção específica e uma maior simplificação do cumprimento do quadro legislativo da União em matéria de cibersegurança (NIS2);

- Um quadro abrangente e horizontal para abordar os riscos de cibersegurança nas cadeias de abastecimento das TIC.[14]

Segundo a CE, esta combinação de opções proporciona «a resposta mais equilibrada e eficaz aos problemas políticos identificados na presente avaliação de impacto». [15]

Embora a CE não exclua completamente outras combinações menos restritivas das suas opções, considera que o seu pacote preferido é o mais adequado, equilibrado e eficaz.

Isto parece sugerir que são possíveis soluções menos radicais e menos intrusivas do que as propostas no pacote preferido, particularmente no que diz respeito ao HRS ou ao quadro relativo aos países de origem com problemas de cibersegurança.

No entanto, o CSA2 contém aspetos que serão certamente sujeitos a um escrutínio minucioso e aprofundado sobre a sua legalidade e fundamentação sólida ao longo do processo legislativo.

Num relatório de junho de 2025, a Comissão da Indústria, Investigação e Energia do Parlamento Europeu salientou que a revisão do CSA se deveria centrar na interação entre soberania e segurança.

Em 5 de janeiro de 2026, o Serviço de Pesquisa Parlamentar do PE publicou um relatório reconhecendo os potenciais desafios relativos à “soberania e aos limites legais da influência da ENISA”.[16] Salienta que a questão mais controversa que divide as partes interessadas e os Estados-Membros é a diferença de opinião entre aqueles que defendem a autonomia digital da UE e aqueles que “dão prioridade aos mercados abertos e à neutralidade técnica”. [17]

Como mencionado anteriormente, isto também pode estar relacionado com a dimensão geoestratégica da cibersegurança,

incluindo a relação com grandes empresas tecnológicas que não estão presentes no mercado interno da UE.

As questões de soberania podem, portanto, ser divididas em duas categorias principais: (i) autonomia estratégica da UE em geral versus grandes empresas tecnológicas supranacionais e (ii) segurança a nível da UE em relação às considerações de segurança nacional dos Estados-Membros da UE.

A exposição de motivos do documento acima referido refere-se ao princípio da subsidiariedade previsto no artigo 5.º do Tratado da União Europeia ("**TUE**") e considera que a UE pode alcançar melhores resultados em matéria de cibersegurança do que os Estados-Membros.

Esta abordagem levanta questões sobre a divisão de poderes entre a UE e os seus Estados-Membros no que diz respeito a questões de segurança nacional. Em primeiro lugar, tal como estabelecido no artigo 5.º, n.º 1, do TUE, o exercício das competências da União é regido pelo princípio da subsidiariedade — a par do princípio da proporcionalidade —, o que pressupõe que a União tenha sido investida da respetiva competência, ao abrigo do princípio da atribuição previsto no mesmo artigo. [18] Em segundo lugar, o artigo 4.º, n.º 2, do TUE, estabelece que "a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro", o que parece implicar que a UE está impedida de tomar medidas sobre essas questões.

De qualquer forma, o novo CSA2 está atualmente a ser negociado como um regulamento entre o Parlamento Europeu e o Conselho, ao

abrigo do processo legislativo ordinário. Não existe, neste momento, uma estimativa precisa de quando poderá ser adotado.

Geoestratégia, autonomia estratégica e segurança nacional

A CSA2 também aborda as questões da soberania e da autonomia estratégica no âmbito dos debates políticos e geoestratégicos globais em curso (com especial enfoque na Europa e na UE), cujo resultado influenciará, sem dúvida, as negociações no âmbito do processo legislativo.

De certa forma, a CSA2 reflete a crescente consciência dos riscos associados à segurança das redes e produtos de comunicação na Europa, particularmente na UE. A gestão de crises híbridas com potencial impacto sistémico é agora a norma, sendo a resiliência cibernética uma questão de segurança, quer a nível dos Estados-Membros quer da União.

Dada a crescente importância da segurança em setores como os transportes, o abastecimento de água, as finanças e a saúde, bem como as suas implicações políticas, a UE enfatiza a necessidade de esforços nacionais coordenados para lidar com o alto nível de interconectividade e os efeitos em cascata das ameaças às cadeias de abastecimento digitais, que podem afetar vários Estados ou mesmo a União como um todo. Isto é conseguido através de legislação como a CSA e a NIS2, bem como de instituições como a ENISA.

Para o efeito, e com vista a reforçar a resiliência da União, os Estados são convidados a desenvolver e aplicar estratégias nacionais que abordem a segurança da cadeia de abastecimento, a gestão da vulnerabilidade e a resposta a incidentes em grande escala.

Em termos de política externa e relações internacionais, porém, é evidente que a dimensão europeia está a tornar-se cada vez mais importante num contexto geoestratégico em rápida mudança. Os interesses de cada Estado-Membro no mercado único e nas comunicações transfronteiriças, essenciais para a implementação das políticas públicas europeias, estão a tornar-se cada vez mais importantes.

Neste contexto, surge a questão da relação da UE com os seus concorrentes e parceiros políticos e económicos. Num ambiente geopolítico e geoeconómico em rápida expansão e altamente volátil, as decisões sobre políticas públicas relativas a parceiros externos — tais como as tarifas dos EUA ou as atividades de grandes empresas tecnológicas na Europa — tornam-se centrais para a geoestratégia europeia e são certamente uma preocupação comum a todos os países da UE.

A UE precisa de parceiros, e é evidente que as alianças e parcerias em que anteriormente confiava já não são eficazes, pelo que tem desenvolvido novos acordos. Esta tendência só se tornará mais pronunciada nos próximos anos.

Neste contexto, a União procura reduzir as suas dependências externas, regulamentar as tecnologias críticas e a sua resiliência e conceber relações estratégicas com os seus concorrentes económicos.

No entanto, as estratégias nacionais em matéria de defesa, informações e inteligência continuam a ser da responsabilidade soberana dos Estados-Membros. Trata-se, evidentemente, de uma questão controversa, mas o Tratado e a jurisprudência apontam nessa direção.

Base jurídica do CSA2 e repartição de competências em matéria de segurança nacional

O princípio da atribuição é um princípio fundamental do direito da EU. Consagrado no artigo 5.º, n.º 2, do TFUE, que constitui uma regra constitucional fundamental de distribuição das competências entre os níveis nacional e da EU, determina que a União só pode agir dentro dos limites das competências que lhe são atribuídas pelos Estados-Membros nos Tratados e que qualquer competência não atribuída permanece com os Estados-Membros.

No caso da segurança nacional, não só o TUE não confere qualquer competência à UE, como também especifica explicitamente, no artigo 4.º, n.º 2, que esta "continua a ser da exclusiva responsabilidade de cada Estado-Membro". Além disso, a salvaguarda da segurança nacional é equiparada a outras "funções essenciais do

Estado", a par da "garantia da integridade territorial do Estado" e da "manutenção da ordem pública".

Tal como salientado pelo TJUE, [19] é prerrogativa dos Estados-Membros tomar as medidas adequadas para manter a lei e a ordem e garantir a segurança interna e externa nos seus territórios, preservando simultaneamente a eficácia do direito da UE, sob um controlo judicial adequado.

Num artigo publicado no EU Law Live intitulado "EU Law and the limits of invoking national security" ("O direito da UE e os limites da invocação da segurança nacional"),[20] José Luís da Cruz Vilaça aborda a interpretação e os limites do conceito de segurança nacional, bem como a compatibilidade das medidas relacionadas com a segurança nacional com o direito da UE.

Neste contexto, a escolha do artigo 114.º do Tratado sobre o Funcionamento da UE («TFUE») como base jurídica para um regulamento como a Lei da Cibersegurança, cujo principal objetivo é a segurança (incluindo a segurança nacional) e não o mercado interno, poderia invalidar todo o regulamento.

A referência ao artigo 114.º do TFUE como única base jurídica poderia ser legitimamente considerada como uma invasão de uma área de competência nacional exclusiva, o que torna difícil conciliar o regulamento proposto com os limites dos poderes da UE, tal como definidos nos Tratados.

A este respeito, a jurisprudência constante do TJUE sustenta que «no contexto da organização dos poderes da UE, a escolha da base

jurídica de uma medida não pode depender simplesmente da convicção de uma instituição quanto ao objetivo prosseguido, mas deve basear-se em fatores objetivos passíveis de controlo jurisdicional». [21]

Deve também ser referido que, durante o processo legislativo de adoção da CSA, alguns parlamentos nacionais manifestaram dúvidas sobre a base jurídica utilizada e a sua aplicação a questões de segurança nacional [22].

Por conseguinte, o legislador da UE deve prestar a devida atenção à preservação de uma separação clara entre as questões que devem ser mantidas sob a exclusiva responsabilidade dos Estados-Membros (aspectos de segurança nacional) e as questões que podem ser abrangidas pelo artigo 114.º do TFUE no que diz respeito à competência da UE para o estabelecimento e o funcionamento do mercado interno (o ecossistema digital), independentemente da dificuldade que possa representar o ajuste da linha divisória. Isso é exigido, acima de tudo, pelo princípio da atribuição.

Esta necessidade é salientada na NIS2, no seu artigo 2.º, n.º 6, onde se afirma expressamente que as suas disposições "não prejudicam" a responsabilidade dos Estados-Membros de salvaguardar a segurança nacional e outras funções essenciais do Estado, tais como a integridade territorial e a manutenção da ordem pública.

De acordo com o dever de fundamentação imposto à administração e ao legislador[23], incluindo a UE e os Estados-Membros quando aplicam o direito da UE, bem como o direito a uma boa administração conferido aos indivíduos ao abrigo do direito da EU,

artigo 41.º, n.º 2, alínea c), da Carta dos Direitos Fundamentais da União Europeia, qualquer ato jurídico deve fornecer uma justificação convincente para a sua intervenção. Isto permite aos cidadãos e às empresas verificar se os limites de competência foram excedidos e exercer o seu direito de recurso judicial. Permite também aos tribunais proceder a essa revisão. Isto aplica-se, evidentemente, ao projeto de CSA.

De acordo com a jurisprudência constante do TJUE[24], meras considerações genéricas são insuficientes para fornecer fundamentos sólidos para a apreciação da legalidade do ato jurídico, de forma a garantir o respeito pelos princípios da atribuição, da segurança jurídica e da previsibilidade. Da mesma forma, a utilização de conceitos vagos, como "HRS" ou "país de risco", exige uma fundamentação clara sobre os seus componentes objetivos.

Proporcionalidade e subsidiariedade

A CE sustenta que a medida proposta está em conformidade com o princípio da proporcionalidade, uma vez que não excede o necessário para atingir os objetivos pretendidos. De acordo com a proposta, o âmbito de intervenção da União não impede novas medidas nacionais no domínio da segurança nacional.

Por conseguinte, a ação da União é justificada tanto do ponto de vista da subsidiariedade como da proporcionalidade.

No entanto, este raciocínio é problemático. O argumento da Comissão reflete a lógica típica da harmonização mínima, segundo a qual a legislação da UE estabelece uma base comum, permitindo simultaneamente aos Estados-Membros manter ou introduzir normas mais rigorosas. Embora esta abordagem possa ser adequada em domínios de competência partilhada, é claramente incompatível com a competência exclusiva dos Estados-Membros no domínio da segurança nacional.

De acordo com o artigo 5.º, n.º 1 TUE, os limites das competências da União são regidos pelo princípio da atribuição. Os princípios da subsidiariedade e da proporcionalidade complementam este princípio, estabelecendo as condições que regem o exercício dessas competências. Em substância, ao abrigo do princípio da proporcionalidade, o conteúdo e a forma da ação da União não devem exceder o necessário para atingir os objetivos estabelecidos nos Tratados.

Por conseguinte, a União só pode agir num determinado domínio político se:

i) a ação se inscrever no âmbito das competências que lhe são atribuídas pelos Tratados (princípio da atribuição, artigo 5.º, n.º 2, do TUE);

(ii) em domínios de competência partilhada, os objetivos da ação proposta não possam ser suficientemente alcançados pelos Estados-Membros isoladamente, mas possam ser melhor alcançados a nível da

União devido à dimensão ou aos efeitos da ação proposta (princípio da subsidiariedade, artigo 5.º, n.º 3, do TUE); e

(iii) o conteúdo e a forma da ação se limitem ao estritamente necessário para atingir os objetivos prosseguidos (princípio da proporcionalidade, artigo 5.º (4) do TUE).

A questão central não é se os Estados-Membros estão autorizados a exceder a medida da União, mas se a União pode intervir, dado que a proposta limita a liberdade dos Estados-Membros de determinar o nível adequado de intervenção em áreas que são da sua competência exclusiva, estabelecendo um limiar regulamentar vinculativo.

Mesmo os requisitos mínimos da União limitam necessariamente a discricionariedade dos Estados-Membros e constituem, por conseguinte, uma intromissão num domínio que lhes é reservado pelos Tratados.

Consequentemente, a proposta corre o risco de criar uma situação em que os Estados-Membros são limitados por uma ação da União que excede a competência da União, não garantindo um equilíbrio adequado e proporcionado entre os objetivos de segurança nacional e os requisitos do mercado interno.

Conclusão

A proposta CSA2 será por certo objeto de longas discussões entre as instituições europeias no centro do processo de tomada de decisão: o Conselho de Ministros, o Parlamento Europeu e a Comissão. Várias disposições serão provavelmente contestadas. Dadas as várias fraquezas da proposta, é improvável que o resultado seja exatamente o proposto pela Comissão.

No cerne da questão está a divisão de competências entre a União e os Estados-Membros, que é particularmente sensível no que diz respeito a questões relacionadas com a segurança nacional.

Pela sua própria natureza, uma proposta sobre cibersegurança tem como "objetivo principal predominante" a segurança nacional dos Estados-Membros da UE (Diretiva Resíduos, referida). Por conseguinte, é da sua competência exclusiva, desde que respeitados os princípios fundamentais do direito da UE, incluindo os direitos fundamentais e os elementos essenciais do mercado interno. Isto implica que as medidas jurídicas neste domínio devem ser devidamente motivadas e sujeitas a controlo jurisdicional.

O artigo 114.º do TFUE fornece uma base jurídica para medidas relativas ao mercado interno, que é uma área de competência partilhada entre a UE e os Estados-Membros. Por conseguinte, não constitui uma base jurídica adequada para uma proposta como a CSA2.

Além disso, a utilização de conceitos como HRS e países de risco, que estão sujeitos à avaliação discricionária da CE, pode criar grande incerteza.

Ao basear-se no princípio da proporcionalidade, a CE está a basear-se numa lógica de harmonização mínima, que é adequada para áreas de competência partilhada. No entanto, a CE está a introduzir erroneamente os princípios da proporcionalidade e da subsidiariedade ao definir os limites da intervenção da UE em áreas fora da sua competência. Ao estabelecer um limiar regulamentar vinculativo, a proposta limita a liberdade dos Estados-Membros de determinar o nível adequado de intervenção em áreas da sua competência exclusiva.

A soberania está, portanto, no centro da controvérsia que esta proposta inevitavelmente causará. Na fase atual de desenvolvimento do direito da UE e à luz da atual turbulência geopolítica, isso pode exacerbar as tensões relativas à relação entre os níveis nacional e da UE. As reservas levantadas por alguns Estados-Membros e diferentes organizações durante as discussões sobre o pacote digital, bem como durante as discussões sobre a CSA original e a Caixa de Ferramentas 5G, são uma expressão dessas tensões.

Nas circunstâncias atuais, e considerando as opções apresentadas em relação aos quatro pilares da CSA2 — ENISA, ECCF, procedimentos simplificados (NIS2) e cadeias de abastecimento seguras de TIC —, seria aconselhável concluir um processo legislativo menos restritivo e mais equilibrado, que respeite os princípios fundamentais que regem a arquitetura constitucional da UE.

Lisboa, 18 de fevereiro de 2026

[1] Regulamento (UE) 2019/881, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança).

[2] Diretiva (UE) 2022/2555, de 14 de dezembro de 2022, relativa a medidas para um nível comum elevado de cibersegurança em toda a União.
[3] O Pacote Digital Omnibus foi apresentado em 19 de novembro de 2025. Tem como objetivo simplificar e racionalizar o quadro regulamentar digital em termos de acesso aos dados, privacidade e cibersegurança. Inclui alterações à Lei da UE relativa aos dados; um ponto único de comunicação para o RGPD, NIS2, DORA e CER; a abolição do regulamento relativo às plataformas para as empresas (P2B); alterações à regra do «consentimento para cookies»; a alteração da definição de dados pessoais e dados de categoria especial; e a autorização do tratamento de dados pessoais para treinar modelos de IA com base num interesse legítimo. Na mesma data, a CE lançou também um Omnibus Digital sobre a Proposta de Regulamentação da IA (AI Omnibus), que altera aspetos da Lei da IA da UE. Os relatórios finais das comissões do PE sobre o pacote, bem como uma «abordagem geral» do Conselho da UE, deverão ser apresentados até ao segundo trimestre de 2026.
[4] Agência da União Europeia para a Cibersegurança.
[5] Ativos TIC essenciais para redes de comunicações eletrónicas móveis e fixas. As infraestruturas críticas em causa são (i) redes de comunicações eletrónicas 5G (não autónomas e autónomas) (ii), redes de comunicações eletrónicas fixas e (iii) redes de comunicações eletrónicas por satélite.
[6] «Fornecedores/vendedores de alto risco» não é uma categoria jurídica consolidada, mas sim uma noção funcional relacionada com fornecedores cuja tecnologia, serviços ou posição na cadeia de abastecimento são considerados pela UE como capazes de ter um impacto sistémico nas infraestruturas críticas, facilitando a exploração de vulnerabilidades técnicas ou criando dependências excessivas de fornecedores de países que estão em risco de interferência estatal e que podem representar um risco elevado para a segurança da UE com base nas suas leis, sistemas jurídicos, práticas ou evidências de atividades cibernéticas maliciosas. Este conceito está definido na «Caixa de Ferramentas 5G», que recomenda que os Estados-Membros excluam estes fornecedores das partes mais sensíveis e críticas das redes de telecomunicações.
[7] Exposição de motivos, página 6.
[8] Idem.
[9] Exposição de motivos, página 3.
[10] Programa de adequação e desempenho regulamentar.
[11] Idem.
[12] Avaliação de impacto, página 39.
[13] Exposição de motivos, p. 12. Ver também pp. 109 *e seguintes* da avaliação de impacto.
[14] Idem.
[15] Idem.
[16] Idem.
[17] Idem.
[18] O artigo 5.º do TUE estabelece: «1. Os limites das competências da União são regidos pelo princípio da atribuição. O exercício das competências da União é regido pelos princípios da subsidiariedade e da proporcionalidade.
2. Nos termos do princípio da atribuição, a União só pode agir dentro dos limites das competências que lhe são atribuídas pelos Estados-Membros nos Tratados para atingir os objetivos neles definidos. As competências não atribuídas à União nos Tratados permanecem com os Estados-Membros.»
[19] Acórdão de 2 de abril de 2020, *Comissão Europeia contra Polónia, Comissão Europeia contra Hungria e Comissão Europeia contra República Checa*, processos apensos C-715/17, C-718/17 e C-719/17, EU:C:2020:257, n.º 143.
[20] Publicado na edição de fim de semana da EU Law Live de 12 de julho de 2025 (n.º 238).
[21] Ver acórdãos de 11 de junho de 1991, C-300/89, *Comissão contra Conselho* (*Diretiva relativa aos resíduos da indústria do dióxido de titânio - Base jurídica*), n.º 10; de 17 de março de 1993, C-155/91, *Comissão contra Conselho (Diretiva relativa aos resíduos)*, n.ºs 7, 19-21. De acordo com este último, «Quando uma medida tem um duplo objetivo, e um deles é identificável como o objetivo principal ou predominante, a medida deve basear-se numa única base jurídica.»
[22] Vg. Senado francês, Parecer Fundamentado, 27/11/2017: «(...) No que diz respeito à competência dos Estados-Membros em matéria de segurança: – o Senado sublinha que a cibersegurança, dada a sua importância para a segurança dos Estados-Membros, é, em vários

aspetos, uma área de soberania nacional; – consequentemente, os Estados-Membros devem manter, por um lado, a sua faculdade de adotar normas e padrões que proporcionem um nível de segurança mais elevado e, por outro lado, o seu lugar de pleno direito no novo dispositivo europeu, com base na sua participação voluntária numa cibersegurança europeia; – por esse motivo, no que diz respeito à base jurídica da proposta, considera que um regulamento sobre cibersegurança não pode apenas tratar do funcionamento do mercado interno (artigos 26.º e 114.º do TFUE), mas também deve integrar questões de segurança (artigo 5.º do Tratado da União Europeia)»; Bundesrat, 15/12/2017: «O Bundesrat duvida que a proposta esteja em conformidade com os princípios da subsidiariedade e da proporcionalidade. Já existem sistemas de certificação comprovados a nível nacional. A exclusão desses sistemas nacionais acarreta o risco de que deixem de poder ser implementados de forma eficaz. Tal ingerência em questões de segurança nacional não é necessária – em vez disso, um sistema de certificação europeu poderia ser complementado por medidas nacionais; República Checa, 12/09/2017: «(…) O Senado (...) Observa que os Estados-Membros são os principais responsáveis pela segurança nacional, incluindo a cibersegurança».

[23] De acordo com o artigo 296.º, segundo parágrafo, do TFUE, «os atos jurídicos devem indicar os motivos em que se baseiam».

Ver também, entre outros, os acórdãos de 4 de julho de 1963, Processo 24-62, *Alemanha contra Comissão*, n.º 69, e de 14 de fevereiro de 1990, C-350/88, *Delacre e.o. contra Comissão*, n.º 15.

[24] Vg., inter alia, 18 de junho de 2015, C-583/13, Deutsche Bahn, n.os 56, 60, 62, 63, 64, 65.