Proposta de Lei n.º 86/XV/1 (GOV)

Adapta a ordem jurídica interna ao Regulamento (UE) 2021/784, relativo ao combate à difusão de conteúdos terroristas em linha

Data de admissão: 25 de maio de 2023

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias (1.ª)

ÍNDICE

Elaborada por: Ana Cláudia Cruz e Gonçalo Sousa Pereira (DAC), Filipa Paixão e Leonor Calvão Borges (DILP), Rafael Silva (DAPLEN) e Rosalina Espinheira (BIB)
Data: 09.06.2023

I. A INICIATIVA

A presente iniciativa visa adaptar a ordem jurídica interna ao Regulamento (UE) 2021/784, relativo ao combate à difusão de conteúdos terroristas em linha, procedendo à designação das entidades competentes, conforme disposto no artigo 12.º, e estabelecendo o regime sancionatório a aplicar em caso de incumprimento, nos termos do artigo 18.º, ambos do Regulamento (UE) 2021/784.

Aponta o proponente que o Regulamento (UE) 2021/784 tem como objetivo garantir o bom funcionamento do Mercado Único Digital numa sociedade aberta e democrática, sendo reconhecida a suscetibilidade dos prestadores de serviços de alojamento virtual para serem utilizados de forma abusiva por terceiros no contexto de atividades ilegais, nomeadamente para difusão de conteúdos terroristas, e impondo-se, por isso, a necessidade de assegurar o equilíbrio entre a segurança jurídica dos prestadores de serviços de alojamento virtual e a confiança dos utilizadores no ambiente virtual.

Reconhecendo a responsabilidade social assumida pelos prestadores de serviços de alojamento virtual no auxílio ao combate dos conteúdos ilegais, o Parlamento Europeu e o Conselho adotaram o Regulamento (UE) 2021/784, cominando aos Estados Membros a consagração de medidas de combate à difusão de conteúdos terroristas em linha.

Asssim, a presente inicitiava, em cumprimento do artigo 12.º do referido Regulamento, vem, no artigo 3.º, designar a Polícia Judiciária como entidade competente para emitir decisões de supressão ou bloqueio e analisar decisões de supressão emitidas por outros Estados-Membros e a Autoridade Nacional de Comunicações (ANACOM) como entidade competente para supervisionar a aplicação das medidas específicas pelos prestadores de serviços de alojamento virtual e aplicar sanções.

Dando cumprimento ao disposto no artigo 18.º do Regulamento, consagra o regime sancionatório aplicável aos prestadores de serviços de alojamento virtual que sejam pessoas singulares, coletivas ou equiparadas, tipificando, no artigo 7.º, as

contraordenações e fixando as respetivas sanções e determinando, no artigo 8.º, que a tentativa e a negligência são puníveis.

Entre outros aspectos procedimentais, estipula que, à tramitação das contraordenações, se aplica o regime quadro das contraordenações no setor das comunicações, aprovado pelo Lei n.º 99/2009, de 4 de setembro, na sua redação atual.

Em concreto, o Projeto de Lei em apreço contém quinze artigos, com as seguintes epígrafes:

- 1.º Objeto;
- 2.º Âmbito de aplicação;
- 3.º Entidades competentes;
- 4.º Impugnação da decisão de supressão ou bloqueio ou de validação de decisão transnacional;
- 5.º Recurso;
- 6.º Responsabilidade pelas contraordenações;
- 7.º Contraordenações;
- 8.º Punibilidade da tentativa e da negligência;
- 9.º Determinação da coima aplicável;
- 10.º Cumprimento do dever omitido;
- 11.º Entidade instrutora;
- 12.º Dever de cooperação;
- 13.º Produto das coimas;
- 14.º Regime aplicável:
- 15.º Alteração à Lei n.º 99/2009, de 4 de setembro.

II. APRECIAÇÃO DOS REQUISITOS CONSTITUCIONAIS, REGIMENTAIS E FORMAIS

- **Conformidade com os requisitos constitucionais e regimentais**

A iniciativa legislativa em análise foi apresentada pelo Governo, no âmbito do seu poder de iniciativa, previsto no n.º 1 do artigo 167.º e na alínea *d*) do n.º 1 do artigo 197.º da Constituição da República Portuguesa (Constituição) e no artigo 119.º do Regimento da Assembleia da República (Regimento)[1]. Reveste a forma de proposta de lei, nos termos do n.º 2 do artigo 119.º do Regimento.

É subscrita pela Ministra da Presidência, em substituição do Primeiro-Ministro, nos termos do n.º 5 do artigo 4.º e do artigo 2.º do Decreto-Lei n.º 32/2022, de 9 de maio,[2] e pela Ministra da Justiça, conforme disposto no n.º 2 do artigo 123.º do Regimento e no n.º 2 do artigo 13.º da Lei n.º 74/98, de 11 de novembro (lei formulário),[3] e ainda pela Ministra Adjunta e dos Assuntos Parlamentares. Foi aprovada em Conselho de Ministros a 13 de abril de 2023, ao abrigo da competência prevista na alínea *c*) do n.º 1 do artigo 200.º da Constituição.

A presente iniciativa legislativa cumpre os requisitos formais elencados no n.º 1 do artigo 124.º do Regimento, uma vez que está redigida sob a forma de artigos, tem uma designação que traduz sinteticamente o seu objeto principal e é precedida de uma exposição de motivos, cujos elementos são enumerados no n.º 2 da mesma disposição regimental.

A apresentação da presente proposta de lei não foi acompanhada por quaisquer estudos, documentos e pareceres que eventualmente a tenha fundamentado, referidos no n.º 3 do artigo 124.º do Regimento[4], e na exposição de motivos não são referidas pelo Governo quaisquer consultas que tenha realizado sobre a mesma - *cfr*. n.º 2 do artigo 6.º do Decreto-Lei n.º 274/2009, de 2 de outubro, que regula o procedimento de consulta de entidades, públicas e privadas, realizado pelo Governo.

[1] Textos consolidados da Constituição e do Regimento disponíveis no sítio da *Internet* da Assembleia da República.
[2] Diploma disponível no sítio da *Internet* do Diário da República Eletrónico. Todas as referências legislativas são feitas para este portal oficial, salvo indicação em contrário.
[3] Texto consolidado da lei formulário disponível no sítio da *Internet* da Assembleia da República.
[4] As «propostas de lei devem ser acompanhadas dos estudos, documentos e pareceres que as tenham fundamentado».

A presente iniciativa legislativa define concretamente o sentido das modificações a introduzir na ordem legislativa e parece não infringir princípios constitucionais, respeitando assim os limites estabelecidos no n.º 1 do artigo 120.º do Regimento.

A proposta de lei em apreciação deu entrada a 24 de maio de 2023, acompanhada da respetiva ficha de avaliação prévia de impacto de género. Foi admitida e baixou na generalidade à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias (1.ª), em conexão com a Comissão de Economia, Obras Públicas, Planeamento e Habitação (6.ª), a 25 de maio, por despacho do Presidente da Assembleia da República. No dia seguinte foi anunciada em sessão plenária.

- **Verificação do cumprimento da lei formulário**

O título da presente iniciativa legislativa traduz sinteticamente o seu objeto, mostrando-se conforme ao disposto no n.º 2 do artigo 7.º da lei formulário.

A iniciativa pretende alterar a Lei n.º 99/2009, de 4 de setembro, que aprova o regime quadro das contra-ordenações do sector das comunicações, pelo que deve ser acrescentado, em sede de especialidade ou redação final, que se trata, à data, da terceira alteração a este ato legislativo, alterado pelas Leis n.º 46/2011, de 24 de junho, e 16/2022, e 16 de agosto, conforme disposto no n.º 1 do artigo 6.º da lei formulário[5].

No que respeita ao início de vigência, o artigo 16.º desta proposta de lei estabelece que a sua entrada em vigor ocorrerá no trigésimo dia após a sua publicação, mostrando-se assim conforme com o previsto no n.º 1 do artigo 2.º da lei formulário, segundo o qual os atos legislativos «entram em vigor no dia neles fixado, não podendo, em caso algum, o início de vigência verificar-se no próprio dia da publicação».

Em caso de aprovação esta iniciativa revestirá a forma de lei, nos termos do n.º 3 do artigo 166.º da Constituição, pelo que deve ser objeto de publicação na 1.ª série do *Diário da República*, em conformidade com o disposto na alínea *c*) do n.º 2 do artigo 3.º da lei formulário.

Nesta fase do processo legislativo, a iniciativa em análise não nos suscita outras questões no âmbito da lei formulário.

[5] «Os diplomas que alterem outros devem indicar o número de ordem da alteração introduzida e, caso tenha havido alterações anteriores, identificar aqueles diplomas que procederam a essas alterações, ainda que incidam sobre outras normas.»

- **Conformidade com as regras de legística formal**

A elaboração de atos normativos da Assembleia da República deve respeitar as regras de legística formal constantes do Guia de legística para a elaboração de atos normativos[6], por forma a garantir a clareza dos textos normativos, mas também a certeza e a segurança jurídicas.

Segundo as regras de legística formal, o título de um ato de alteração deve referir o ato alterado [7], pelo que do mesmo deve constar a alteração ao regime quadro das contra-ordenações do sector das comunicações. Esta informação deve ainda ser acrescentada na norma sobre o objeto, com os elementos previstos no n.º 1 do artigo 6.º da lei formulário, *supra* referidos.

De referir que a regra de legística formal, segundo a qual os numerais ordinais devem ser sempre redigidos por extenso [8], deve ser aplicada na norma de entrada em vigor, ou seja, deve ser redigido «trigésimo dia».

A iniciativa em apreço não nos suscita outras questões pertinentes no âmbito da legística formal, na presente fase do processo legislativo, sem prejuízo de análise mais detalhada a ser efetuada no momento da redação final.

III. ENQUADRAMENTO JURÍDICO NACIONAL

De acordo com a ficha temática sobre a União Europeia disponível no portal do Parlamento Europeu, sobre o tema «A ubiquidade do Mercado Único Digital», «o Mercado Único Digital visa essencialmente a supressão das barreiras nacionais às transações em linha», tendo «potencial para melhorar o acesso à informação, trazer benefícios à eficiência em termos de custos reduzidos das transações, consumo desmaterializado e menor pegada ecológica e introduzir melhores modelos empresariais e administrativos».

[6] Documento disponível no sítio da *Internet* da Assembleia da República
[7] DUARTE, David [*et al.*] – *Legística: perspectivas sobre a concepção e redacção de actos normativos*. Coimbra : Almedina, 2002. P. 201.
[8] DUARTE, David [*et al.*] – *Legística: perspectivas sobre a concepção e redacção de actos normativos*. Coimbra : Almedina, 2002. P. 166. *Guia de legística para a elaboração de atos normativos* : Divisão de Edições da Assembleia da República, 2020. P. 40.

Consta ainda na referida ficha temática que «o Mercado Único Digital foi reconhecido como uma prioridade pela Comissão Europeia na sua Estratégia para o Mercado Único Digital (COM(2015)0192[9]) e, recentemente, no Programa para a Europa 2019-2024 da presidente da Comissão».

A Lei n.º 27/2021, de 17 de maio[10], aprovou a Carta Portuguesa de Direitos Humanos na Era Digital.

De acordo com o artigo 2.º deste diploma «a República Portuguesa participa no processo mundial de transformação da Internet num instrumento de conquista de liberdade, igualdade e justiça social e num espaço de promoção, proteção e livre exercício dos direitos humanos, com vista a uma inclusão social em ambiente digital» (n.º 1), prevendo-se ainda na mesma norma que «as normas que na ordem jurídica portuguesa consagram e tutelam direitos, liberdades e garantias são plenamente aplicáveis no ciberespaço» (n.º 2).

Por seu lado, estabelece o n.º 1 do artigo 4.º que «todos têm o direito de exprimir e divulgar o seu pensamento, bem como de criar, procurar, obter e partilhar ou difundir informações e opiniões em ambiente digital, de forma livre, sem qualquer tipo ou forma de censura, sem prejuízo do disposto na lei relativamente a condutas ilícitas». Esta norma acrescenta no n.º 4 que «todos têm o direito de beneficiar de medidas públicas de promoção da utilização responsável do ciberespaço e de proteção contra todas as formas de discriminação e crime, nomeadamente contra a apologia do terrorismo, o incitamento ao ódio e à violência contra pessoa ou grupo de pessoas por causa da sua raça, cor, origem étnica ou nacional, ascendência, religião, sexo, orientação sexual, identidade de género ou deficiência física ou psíquica, o assédio ou exploração sexual de crianças, a mutilação genital feminina e a perseguição».

A Lei n.º 52/2003, de 22 de agosto, tem como objeto a previsão e a punição dos atos e organizações terroristas, transpondo para a ordem jurídica interna a Diretiva (UE)

[9] Texto retirado do portal legislativo da União Europeia EUR-LEX. Consultas efetuadas a 30/05/2023.
[10] Texto consolidado retirado do sítio da Assembleia da República. Todas as referências legislativas relativas à Constituição são feitas para este portal oficial, salvo indicação em contrário. Consultas efetuadas a 30/05/2023.

2017/541, do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo, e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho.

Nos termos do n.º 1 do artigo 2.º, «considera-se grupo terrorista a associação de duas ou mais pessoas que, independentemente de ter ou não funções formalmente definidas para os seus membros, continuidade na sua composição ou estrutura elaborada, se mantém ao longo do tempo e atua de forma concertada com o objetivo de cometer infrações terroristas», entendendo-se como infrações terroristas os atos discriminados nas várias alíneas da norma (como sejam, as ofensas à vida ou à integridade física, a captura de aeronaves, navios ou outros meios de transporte coletivo ou de mercadorias, a perturbação ou a interrupção de recurso natural fundamental que crie perigo para as vidas humanas, entre outros), «na medida em que estejam previstos como crime, que, pela sua natureza ou pelo contexto em que são cometidos, possam afetar gravemente o Estado, um Estado estrangeiro ou uma organização internacional, quando forem praticados com o objetivo de intimidar gravemente certas pessoas, grupos de pessoas ou a população em geral, compelir de forma indevida os poderes públicos ou uma organização internacional a praticar ou a abster-se de praticar um ato ou de perturbar gravemente ou destruir as estruturas políticas, constitucionais, económicas ou sociais fundamentais do Estado, de um Estado estrangeiro ou de uma organização internacional».

De acordo com o n.º 1 do artigo 4.º deste diploma, «quem praticar uma infração terrorista é punido com pena de prisão de 2 a 10 anos ou com a pena correspondente ao crime praticado, agravada de um terço nos seus limites mínimo e máximo, se for igual ou superior àquela». Pune igualmente o n.º 3 da norma, com uma pena de prisão de 1 a 5 anos, «quem, defendendo, elogiando, incentivando ou apelando à prática de infrações terroristas, por qualquer meio distribuir ou difundir mensagem ao público que incite à prática das infrações terroristas». Por fim, determina ainda o n.º 4 deste artigo 4.º que, sempre que os factos previstos no n.º 3 «forem praticados através de meios de comunicação eletrónica, acessíveis por Internet, o agente é punido com pena de prisão de 1 a 6 anos».

Em anexo à Resolução do Conselho de Ministros n.º 40/2023, de 3 de maio, foi aprovada a Estratégia Nacional de Combate ao Terrorismo.

Esta Estratégia «está organizada em torno de quatro eixos estratégicos - prevenir, proteger, perseguir e responder - cuja materialização assenta na contínua implementação dos diversos planos de ação em vigor, bem como na definição de outras medidas concretas» (ponto 3).

No eixo «Prevenir»[11] uma das linhas de ação delineadas é a de «coordenar todas as capacidades necessárias para combater os discursos de ódio e a desinformação no ciberespaço, bem como noutros espaços comunicacionais comuns globais, inviabilizando a sua instrumentalização para a radicalização, captação e recrutamento de indivíduos e para a difusão de propaganda extremista» [viii)].

Por seu lado, no eixo «Perseguir»[12] define-se, entre outras linhas de ação, a garantia dos «meios apropriados para perseguir a utilização do ciberespaço para apoiar e financiar o terrorismo e promover o recrutamento, radicalização e disseminação de propaganda violenta» [v)].

O Decreto-Lei n.º 137/2019, de 13 de setembro, aprovou a nova estrutura organizacional da Polícia Judiciária (PJ), definindo-a como «um corpo superior de polícia criminal organizado hierarquicamente na dependência do membro do Governo responsável pela área da justiça e fiscalizado nos termos da lei» (n.º 1 do artigo 1.º). Trata-se de «um serviço central da administração direta do Estado, dotado de autonomia administrativa» (n.º 2 da mesma norma).

De acordo com o artigo 18.º deste diploma, o qual regula a estrutura orgânica da PJ, uma das unidades centrais de investigação criminal desta entidade é a Unidade Nacional Contraterrorismo (UNCT) [alínea a) do n.º 3].

[11] O qual visa antecipar e detetar potenciais ameaças terroristas, conhecendo e identificando as causas e tendências que determinam o surgimento de processos de radicalização, adesão e recrutamento, de modo a prevenir atos que configurem infrações terroristas.
[12] O qual visa impedir a ocorrência de atos terroristas, assente no esforço de prevenção direcionado para a deteção e investigação criminal de todas as infrações terroristas, infrações relacionadas com grupos terroristas, infrações relacionadas com atividades terroristas e financiamento do terrorismo, por forma a impedir o planeamento e execução de ações hostis, neutralizar fontes de apoio logístico e redes de financiamento, responsabilizando-as criminalmente.

A UNCT vem regulada de forma detalhada no artigo 30.º deste decreto-lei.

O Decreto-Lei n.º 39/2015, de 16 de março, aprovou, em anexo, os estatutos da Autoridade Nacional de Comunicações (ANACOM).

No artigo 1.º dos referidos Estatutos, determina-se que a ANACOM «é uma pessoa coletiva de direito público, com a natureza de entidade administrativa independente, dotada de autonomia administrativa, financeira e de gestão, bem como de património próprio» (n.º 1), que «tem por missão a regulação do setor das comunicações, incluindo as comunicações eletrónicas e postais e, sem prejuízo da sua natureza, a coadjuvação ao Governo no domínio das comunicações» (n.º 2).

Prevê-se no artigo 8.º que, enquanto entidade reguladora, cabe à ANACOM, entre outros, «promover a concorrência na oferta de redes e serviços» [alínea a) do n.º 1], «garantir o acesso a redes, infraestruturas, recursos e serviços» [alínea b) do n.º 1], «assegurar a garantia da liberdade de oferta de redes e de prestação de serviços» [alínea c) do n.º 1], ou, «proteger os direitos e interesses dos consumidores e demais utilizadores finais» [alínea h) do n.º 1].

Ainda de referir é o que se estabelece no n.º 1 do artigo 9.º do diploma, nos termos do qual «para prosseguir as suas atribuições, a ANACOM dispõe de poderes de regulamentação, supervisão, fiscalização e sancionatórios».

A Lei n.º 99/2009, de 4 de setembro, aprova o regime quadro das contraordenações do sector das comunicações.

No n.º 3 do artigo 1.º deste diploma elencam-se exemplificativamente os diplomas legais que regulam matérias que devem considerar-se como integrando o setor das comunicações.

Por fim, refira-se que a Lei n.º 11/2023, de 22 de março, autorizou o Governo a legislar em matéria de direito de autor e direitos conexos no mercado único digital, transpondo a Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019.

IV. ENQUADRAMENTO JURÍDICO NA UNIÃO EUROPEIA E INTERNACIONAL

- **Âmbito da União Europeia**

O Regulamento (UE) 2021/784 do Parlamento Europeu e do Conselho, de 29 de abril de 2021, relativo ao combate à difusão de conteúdos terroristas em linha foi escrutinado pela Assembleia da República.

Com efeito, este Regulamento veio estabelecer regras no plano da União Europeia destinadas a combater a utilização abusiva dos serviços de alojamento virtual para a difusão ao público de conteúdos terroristas[13] em linha, abrangendo os prestadores de serviços de alojamento virtual (PSAV)[14] no combate à difusão ao público de conteúdos terroristas através dos seus serviços assegurarando, se necessário, que esses conteúdos sejam suprimidos bem como as medidas a adotar pelos Estados-Membros para a identificação de conteúdos terroristas permitindo a sua supressão de forma expedita pelos PSAV[15], e facilitar a cooperação entre as autoridades competentes dos Estados-Membros, os PSAV e, se for o caso, a Europol.

Acresce que, este Regulamento define, igualmente, um conjunto de medidas destinadas a combater a difusão ao público de conteúdos terroristas em linha, nomeadamente, através de decisões de supressão onde os PSAV destinatários de uma decisão têm de suprimir ou bloquear os conteúdos em questão no prazo de uma hora; procedimentos de supressão transfronteiriços — isto é, quando o PSAV não está localizado no mesmo Estado-Membro que a autoridade nacional que emitiu a decisão de supressão; medidas específicas a adotar pelos PSAV expostos a este tipo de conteúdos; como ainda a conservação desses conteúdos pelos PSAV para efeitos administrativos ou judiciais.

Por fim, tal como focado na iniciativa em análise, destacar que o artigo 12.º do Regulamento supra identificado prevê que «cada Estado-Membro designa a autoridade ou autoridades competentes para: a) emitir decisões de supressão nos termos do artigo

[13] O termo «infrações terroristas» está definido na Diretiva (UE) 2017/541 relativa à luta contra o terrorismo.
[14] Prestador de serviços de alojamento virtual: entidades que efetuam a armazenagem das informações fornecidas por um fornecedor de conteúdos a pedido deste.
[15] O regulamento é aplicável aos PSAV que prestem serviços na UE, quer possuam ou não o seu estabelecimento principal num Estado-Membro.

3.º [16]; b) analisar decisões de supressão nos termos do artigo 4.º [17]; c) supervisionar a aplicação das medidas específicas nos termos do artigo 5.º [18]; e d) impor sanções nos termos do artigo 18.º» como ainda destacar o artigo 18.º onde é estipulado que os Estados-Membros devem estabelecer «o regime de sanções aplicáveis às infrações ao presente regulamento pelo prestador de serviços de alojamento virtual».

Com efeito, o artigo 18.º concretiza que os Estados-Membros devem assegurar que «as autoridades competentes, ao decidirem da oportunidade de impor uma sanção e ao determinarem o tipo e o nível das sanções, tenham em conta todas as circunstâncias pertinentes, nomeadamente: a) a natureza, a gravidade e a duração da infração; b) o facto de a infração ter sido intencional ou negligente; c) as anteriores infrações cometidas pelo prestador de serviços de alojamento virtual; d) a capacidade financeira do prestador de serviços de alojamento virtual; e) o grau de cooperação do prestador de serviços de alojamento virtual com as autoridades competentes; f) a natureza e a dimensão do prestador de serviços de alojamento virtual, em especial se esse prestador é uma micro, pequena ou média empresa; e g) o grau de dolo do prestador de serviços de alojamento virtual, tendo em conta as medidas técnicas e organizativas tomadas pelo prestador de serviços de alojamento virtual para dar cumprimento ao presente regulamento».

[16] Artigo 3. º do Regulamento (UE) 2021/784
1. A autoridade competente de cada Estado-Membro deve dispor de poderes para emitir decisões de supressão pelas quais solicita aos prestadores de serviços de alojamento virtual que suprimam os conteúdos terroristas ou bloqueiem o acesso aos mesmos em todos os Estados-Membros.

[17] Artigo 4. º do Regulamento (UE) 2021/784
1. Sem prejuízo do artigo 3.º , se o estabelecimento principal ou o representante legal do prestador de serviços de alojamento virtual não estiver localizado no Estado-Membro da autoridade competente que emitiu a decisão de supressão, esta apresenta, em simultâneo, uma cópia da decisão de supressão à autoridade competente do Estado-Membro em que estiver localizado o estabelecimento principal do prestador de serviços de alojamento virtual ou em que residir ou estiver estabelecido o seu representante legal.

[18] Artigo 5. º do Regulamento (UE) 2021/784
1. Os prestadores de serviços de alojamento virtual expostos a conteúdos terroristas a que se refere o n. o 4, devem, se for caso disso, integrar nos seus termos e condições e aplicar disposições para combater a utilização abusiva dos seus serviços para a difusão ao público de conteúdos terroristas.

- **Âmbito internacional**

Países analisados

FRANÇA

Este país aprovou já a *Loi du 16 août 2022*[19] *portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne,* que altera a *loi du 21 juin 2004 pour la confiance dans l'économie numérique* (LCEN).

O diploma designa as seguintes autoridades competentes em França:
O *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication*[20] (OCLCTIC), que depende da direção da polícia judiciária, para emitir injunções nacionais de retirada ou bloqueio no âmbito do regulamento;
A *Autorité de régulation de la communication audiovisuelle et numérique*[21] (ARCOM) para receber a transmissão de todas as injunções e para investigar as injunções transfronteiriças, podendo examinar a conformidade destas injunções transfronteiriças no que diz respeito ao regulamento europeu "TCO" e à Carta dos Direitos Fundamentais da UE. A ARCOM terá ainda que supervisionar os *web hosts* localizados principalmente na França ou têm um representante legal lá e as medidas preventivas às custas das plataformas consideradas expostas.

A lei especifica ainda:
- as penalidades criminais incorridas pelos anfitriões que não cumprem a obrigação de remover ou bloquear ou que não informam às autoridades sobre conteúdo terrorista que "apresentem uma ameaça iminente à vida" ou a anunciar um plano de ataque (um ano de prisão e uma multa de 250.000 euros, e para pessoa colectiva multa até 4% do seu volume de negócios mundial em caso de infracções persistentes);

[19] Texto retirado do portal legislativo francês Legifrance.fr. Todas as referências legislativas relativas a França são feitas para este portal oficial, salvo indicação em contrário. Consultas efetuadas a 2/06/2023.
[20] Portal oficial, disponível aqui: https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite. Consulta efetuada a 2/06/2023.
[21] Portal oficial, disponível aqui: https://www.arcom.fr/. Consulta efetuada a 2/06/2023.

- as penalidades administrativas e financeiras que a ARCOM pode pronunciar (notificação formal para um host cumprir as obrigações dos regulamentos europeus e, em caso de descumprimento, multa de até 4% do seu faturamento mundial).

Os hosts ou internautas que originarem o conteúdo poderão interpor suspensão provisória ou liberdade provisória e interpor recurso de cancelamento até 48 horas perante o tribunal administrativo, que terá 72 horas para decidir. O recurso pode ser interposto no prazo de 10 dias. O tribunal administrativo de recurso terá então um mês para decidir.

A lei integra os novos mecanismos da regulamentação europeia, sem alterar ou suprimir nada dos instrumentos jurídicos já existentes, que se terão, portanto, de articular. De facto, e desde 2015, o *Code de la sécurité intérieure* prevê um procedimento administrativo único que tornou possível bloquear ou excluir conteúdos terroristas.

De acordo com a *loi du 21 juin 2004 pour la confiance dans l'économie numérique* (LCEN) a OCLCTIC pode solicitar aos editores e *hosts* que removam este tipo de conteúdos, após os relatórios feitos através da plataforma Pharos[22], um Portal oficial para denúncia de conteúdo ilegal da Internet.

Cumpre ainda mencionar a chamada lei "Avia", *Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet* reforçou as penalidades em caso de violação dessas obrigações.

V. ENQUADRAMENTO PARLAMENTAR

- **Iniciativas pendentes (iniciativas legislativas e petições)**

Consultada a base de dados da Atividade Parlamentar (AP), verifica-se que, sobre a matéria em causa, não se encontram iniciativas pendentes, nem petições.

- **Antecedentes parlamentares (iniciativas legislativas e petições)**

Na presente Legislatura foi apreciada, sobre «terrorismo», a Proposta de Lei n.º 29/XV/1.ª (GOV) - *Conclui a transposição da Diretiva (UE) 2017/541, alterando designadamente a Lei n.º 52/2003, de 22 de agosto (Lei de Combate ao Terrorismo)*, a

[22] Portal oficial, disponível aqui: https://www.internet-signalement.gouv.fr/PharosS1/. Consulta efetuada a 2/06/2023.

qual deu origem à Lei n.º 2/2023, de 16 de janeiro, *Completa a transposição da Diretiva (UE) 2017/541, alterando a Lei de Combate ao Terrorismo, o Código Penal, o Código de Processo Penal e legislação conexa.*

VI. CONSULTAS E CONTRIBUTOS

Em 31 de maio de 2023, a Comissão solicitou parecer escrito sobre esta iniciativa ao Conselho Superior do Ministério Publico, ao Conselho Superior da Magistratura, à Ordem dos Advogados e à ANACOM - Autoridade Nacional de Comunicações.

Todos os pareceres e contributos remetidos à Assembleia da República serão publicados na página da iniciativa na *Internet*.

VII. AVALIAÇÃO PRÉVIA DE IMPACTO

- **Avaliação sobre impacto de género**

O preenchimento, pelo proponente, da ficha de avaliação prévia de impacto de género da presente iniciativa, em cumprimento do disposto na Lei n.º 4/2018, de 9 de fevereiro, devolve como resultado uma valoração neutro do impacto de género, o que se considera consentâneo com teor da iniciativa, parecendo apontar para que, no entendimento da proponente, o género não é afetado pela aplicação das normas a aprovar, o que não pode deixar de relevar para o juízo a fazer pelos Deputados, na apreciação da iniciativa.

Na verdade, tal valoração é imposta pela Lei n.º 4/2018, de 9 de fevereiro, que determina que a valoração do impacto de género – positiva, neutra ou negativa – visa assegurar a quantificação ou qualificação dos efeitos da norma no que respeita à igualdade entre homens e mulheres, podendo resultar em "*propostas de melhoria ou recomendações, quanto à redação do projeto ou quanto às medidas tendentes à sua execução*" (artigos 10.º a 12.º da Lei).

O juízo dos proponentes no sentido da neutralidade de impacto de género da presente iniciativa é um dos três resultados possíveis da avaliação de impacto imposta por Lei e

a sua consideração parece coincidir com o entendimento de que o objeto da iniciativa em apreço não é propício a afetar a igualdade de género.

VIII. ENQUADRAMENTO BIBLIOGRÁFICO

CANDAU, Javier – **Ciberseguridad** [Em linha] : **evolución y tendências**. Madrid : Instituto Español de Estudios Estratégicos, 2021. [Consult. 2 jun. 2023]. Disponível em WWW:<URL:https://catalogobib.parlamento.pt:82/images/winlibimg.aspx?skey=&doc=136807&img=24863&save=true>.

Resumo: Os desafios que enfrentamos com o constante desenvolvimento da sociedade da informação neste século XXI estão intimamente ligados ao conceito de cibersegurança. Neste artigo o autor analisa a evolução dessa ideia de segurança da informação e da sua regulamentação conforme a tecnologia e as ameaças foram mudando. Ameaças cuja evolução é também analisada e «cujas consequências tornaram inevitável o objetivo de garantir e implementar a segurança no ciberespaço, respeitando a privacidade e a liberdade dos indivíduos.»

Este tem sido o entendimento dos principais governos que fizeram da cibersegurança uma das suas prioridades estratégicas, devido ao seu impacto direto na segurança nacional, na competitividade das empresas e na prosperidade da sociedade como um todo.

Neste artigo é analisada a situação em Espanha, afirmando o autor que «embora a transformação digital fosse já um desafio que as organizações tinham de enfrentar com maior ou menor urgência, a eclosão da pandemia de COVID-19 em 2020 levou à necessidade de adaptar rapidamente os recursos tecnológicos e humanos a esta nova realidade, […] realidade que será marcada nos próximos anos pelo desenvolvimento da Estratégia Nacional de Cibersegurança, o novo esquema nacional de segurança que está em processo de aprovação, e que conta com a participação de atores públicos e privados, para implementar e facilitar um ciberespaço seguro e confiável.»

COCCHINI, Andrea – Ciberdiligencia debida : una actualización necesaria para el Derecho Internacional del ciberespacio? **Análisis del Real Instituto Elcano** [Em linha]

. Madrid. N.º 27 (2021), 6 p. [Consult. 2 jun. 2023]. Disponível em WWW:<URL: https://catalogobib.parlamento.pt:82/images/winlibimg.aspx?skey=&doc=134580&img=21623&save=true>.

Resumo: Para o autor deste estudo «se já é tecnicamente difícil atribuir um ciberataque a um grupo de ciberatacantes que operam no território de outro Estado, não é mais fácil atribuí-lo juridicamente devido à regulamentação internacional aplicável ao ciberespaço.» Partindo desta premissa o autor estuda as dificuldades que existem para atribuir um ciberataque de acordo com os instrumentos de Direito Internacional atualmente disponíveis. Sugere, então, o recurso ao padrão da "diligência cibernética", que implicaria para cada Estado a obrigação de prevenir, através de atividades de monitorização possíveis ameaças cibernéticas de grupos privados sediados no território de um Estado.

CRUZ, Alfredo Pereira da – Cyberwar : a ameaça invisível. **Revista militar**. Lisboa. ISSN 0873-7630. Vol. 73, nº 8/9 (ago./set. 2021), p. 609-624. Cota : RP-401

Resumo: Neste artigo o Tenente-general Piloto Aviador Alfredo Cruz analisa o ciberespaço, definindo-o como «o grande oceano onde confluem os rios da informação e os vários "*bits e bites*" dos sistemas computacionais.» Diz o autor que «é neste espaço volátil que se movimentam as organizações públicas e privadas, as instituições militares, os sistemas financeiros, a economia, os serviços de saúde, o comércio, os serviços públicos e privados, mas também as organizações criminosas, terroristas, de espionagem e subversivas. É aqui no Cyberspace que acontece a Cyberwar.»

"Há trinta anos atrás, o Cyherspace era apenas um termo utilizado para descrever a rede nascente de computadores interligados a meia dúzia de laboratórios universitários. Com o avanço exponencial da tecnologia, o mundo modificou-se vertiginosamente. Modernamente, aquilo que definimos como o "Domínio do Cyberspace" é o conjunto dos computadores, das redes que os interligam e os sistemas de comunicação onde se apoiam.»

Ao longo do artigo o Tenente-general explica, «de forma sintética, como funciona, a sua importância e o que todos nós podemos fazer para que as redes por onde correm e

fluem as informações continuem a desempenhar a sua função em perfeitas condições de credibilidade e confiança.»

CYBER TERRORISM and extremism as threat to critical infrastructure proteccion [Em linha] . Ljubljana : Republic of Slovenia. Ministry of Defense, 2020. [Consult. 2 jun. 2023]. Disponível em WWW:<URL:https://catalogobib.parlamento.pt:82/images/winlibimg.aspx?skey=&doc=133181&img=19555&save=true>.

Resumo: Para os autores deste artigo, o ambiente de segurança global está a tornar-se cada vez mais complexo. «Se as ameaças modernas à segurança representadas pelo terrorismo internacional e pela radicalização associada de indivíduos ou grupos são, de facto, tão complexas como o conteúdo desta publicação descreve, justifica-se fazer várias perguntas, tais como: o que pode um Estado moderno fazer pelo seu sistema de segurança nacional para responder rápida e eficazmente às ameaças terroristas; como deve ser estruturado o sistema nacional de luta contra o terrorismo; que papéis e poderes têm as autoridades de segurança de cada Estado neste sistema; e, especialmente, são as instituições de segurança e outras instituições do Estado adequadamente estruturadas, preparadas e equipadas para serem capazes de levar a cabo as atividades de combate a ameaças, como o terrorismo?» [...] O objetivo desta publicação é encontrar respostas para algumas das perguntas acima. A combinação de diferentes abordagens, conceitos e análises de diferentes casos, bem como o papel das entidades de segurança nacional na luta contra o terrorismo, proporcionam soluções específicas para a maioria das questões, incluindo a cibersegurança e a proteção das infraestruturas críticas, o que, no entanto, não exclui outras considerações científicas e profissionais.

ESTRATÉGIA DE SEGURANÇA nacional : Portugal horizonte 2030. Coimbra : Almedina , 2018. 190 p. ISBN 978-972-40-7458-0. Cota: 08.21 – 120/2018

Resumo: «Os desafios do mundo atual exigem um grande esforço de adaptação das estruturas do Estado às mudanças no ambiente de segurança, de modo a preservar a paz e a segurança nacional. Em Portugal, não existe uma Estratégia de Segurança

Nacional que materialize esse consenso. Este livro propõe uma nova arquitetura do sistema de segurança nacional, alicerçada na criação de um Conselho de Segurança Nacional e na aprovação de uma Lei de Segurança Nacional.»

EUROPEAN INVESTMENT BANK – **European Cybersecurity Investment Platform** [Em linha] . Luxembourg : EIB, 2022. [Consult. 2 jun. 2023]. Disponível em WWW:<URL:https://catalogobib.parlamento.pt:82/images/winlibimg.aspx?skey=&doc=141567&img=29790&save=true>.

Resumo: Neste relatório são apresentados os resultados de um estudo de mercado independente, os quais permitem fazer uma avaliação da necessidade e da procura de produtos financeiros e não financeiros para apoiar o crescimento do setor da cibersegurança na Europa. Com base nas características de mercado identificadas e nas necessidades associadas, o presente relatório avalia os potenciais benefícios e descreve a conceção de uma Plataforma Europeia de Investimento em Cibersegurança (ECIP) específica para apoiar o setor da cibersegurança em toda a Europa. Apresenta igualmente recomendações sobre possíveis fontes de financiamento a nível nacional e europeu, incluindo potenciais vias de desenvolvimento e implementação.

FREITAS, Pedro Miguel – Ciberterrorismo e a Lei do combate ao terrorismo. **Nação e defesa**. Lisboa. ISSN 0870-757X. Nº 161 (abril 2022), p. 115-130. Cota: RP-72

Resumo: Partindo de uma análise da doutrina internacional em torno da conceptualização do ciberterrorismo, o autor pretende com este artigo «aferir se a Lei n.º 52/2003 prevê e pune também esta forma de aparecimento de terrorismo. As inúmeras aceções de ciberterrorismo podem ser reconduzidas a ciberterrorismo em sentido estrito ou ciberterrorismo em sentido amplo. A lei portuguesa, ainda que não tomando uma posição evidente sobre esta distinção, consagra a previsão e punição de ambas as modalidades.»