Ciberterrorismo e a Lei de Combate ao Terrorismo

Pedro Miguel Freitas

Doutorado em Ciências Jurídicas Públicas, ramo de Ciências Criminais, pela Escola de Direito da Universidade do Minho. Docente e Investigador na área das Ciências Criminais e Direito e Novas Tecnologias na Universidade Católica Portuguesa. Membro fundador do Instituto Lusófono de Justiça Criminal. Colaborou na lecionação de cursos organizados pela Universidade de Massachusetts Lowell (EUA), Universidade de Turim (Itália), Universidade Politécnica de Valência (Espanha), Universidade Jean Piaget (Angola), entre outras. É autor de diversas publicações científicas e conferencista em vários eventos científicos, nacionais e internacionais.

Resumo

Partindo de uma análise da doutrina internacional em torno da conceptualização do ciberterrorismo, pretende-se 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.

Palavras-chave: Terrorismo; Ciberterrorismo; Ciberespaço; Internet.

Abstract

Cyber-terrorism and the Counter-Terrorism Act

Starting from an analysis of the international doctrine on the conceptualization of cyber-terrorism, the aim of this article is to assess whether Law no. 52/2003 also foresees and punishes this form of terrorism. The countless meanings of cyberterrorism may be reconducted to cyberterrorism in a strict sense or cyberterrorism in a broad sense. The Portuguese law, although not taking a clear position on this distinction, foresees and punishes both modalities.

Keywords: *Terrorism; Cyberterrorism; Cyberspace; Internet.*

Artigo recebido: 04.04.2022
Aprovado: 19.04.2022
https://doi.org/10.47906/ND2022.161.06

Introdução

O fenómeno do terrorismo é complexo, poliédrico e permeável ao tempo e espaço. Em parte, reside aqui, no seu lastro histórico – do *regime de la terreur* ao terrorismo contemporâneo –, a explicação para a ausência de uma definição consensual do que seja terrorismo. No contexto de uma longevidade assinável, o terrorismo corporizou-se em manifestações que nem sempre se revestiram de idênticas características, pois se mostraram sensíveis às específicas condições sociopolíticas, jurídicas e culturais da época. Estas dissonâncias historicamente propiciadas geraram dúvidas e incertezas, ainda hoje presentes, sobre os seus exatos contornos.
Acresce igualmente que a existência e feições do terrorismo dependem em grande medida do seu observador, pois "a própria palavra torna-se um teste decisivo para crenças arraigadas, de modo que uma breve conversa sobre assuntos terroristas com quase qualquer pessoa revela uma visão de mundo especial, uma interpretação da natureza do homem e um vislumbre de um futuro desejado" (Bell, 1978). Ideia que se percebe de forma cristalina na consagrada expressão "aquele que é terrorista para uma pessoa é combatente da liberdade para outra" (Laqueur, 1987).

1. As Feições do Ciberterrorismo

Um consenso em torno do que o terrorismo é traz consigo um alinhamento, por mínimo que seja, de entendimentos em domínios que são inerentemente polarizadores como a religião, a ideologia ou a política. Não é por isso de todo surpreendente que, diante de esta dificuldade conceptual (Marsili, 2019), apelidada por Brian Jenkins (2004) de "triângulo das Bermudas" onde "conferências inteiras se afundaram sem deixar rasto", se assista a um certo fatalismo e resignação por parte de certa doutrina (Schmid. 2004).
Uma das suas vozes mais audíveis é Walter Laqueur. Nas suas palavras, "[n] enhuma definição abrangente jamais será encontrada pela simples razão de que não há um terrorismo, mas houve muitos terrorismos, muito diferentes no tempo e no espaço, na motivação e nas manifestações e objetivos" (Laqueur, 2007).
Sinteticamente, serão seis os argumentos explicativos desta dificuldade conceptual de terrorismo: complexidade do fenómeno; confusão acerca de relação entre terror e terrorismo; multiplicidade de alvos; diversidade de públicos para quem os atos terroristas são praticados; confusão entre terrorismo e demais formas de violência política; e a multiplicação de tipos de terrorismo (Alex Schmid, 2020).
Em certa medida, o reconhecimento da dificuldade – ou mesmo impossibilidade – de definição do terrorismo aparenta ser contraintuitivo. "A maioria das pessoas", diz-nos Gus Martin (2011), "tem um entendimento instintivo de que o terrorismo é

violência politicamente motivada, usualmente dirigida a alvos fáceis, isto é, alvos civis ou pertencentes a entidades governamentais administrativas, com uma intenção de afetar (aterrorizar) um público-alvo". Isto é, para o cidadão comum não se apresentará como particularmente difícil dizer o que constitui terrorismo. No entanto, esta aparente facilidade esbarra com a realidade da sua operacionalização, ou melhor, a tentativa da sua concretização. Apodítico neste sentido é o estudo de Alex Schmid e Albert Jongman (2005) onde foram reunidas 109 definições de terrorismo e identificados 22 elementos definitórios que se repetiam nessas definições, por exemplo, violência (em 83,5% das definições), político (65%), terror/medo (51%), ameaça (47%), entre outros. Anos mais tarde, o mesmo Alex Schmid (2011) apresenta uma nova lista de definições, que desta vez ultrapassa as 250.

A falta de uma definição consensual do terrorismo acarreta consequências negativas. Ben Saul (2021) aponta essencialmente duas: o declínio na eficiência da investigação e repressão do terrorismo; inconsistência com o direito internacional humanitário e o direito internacional dos direitos humanos.

Com a primeira das referências, o que o autor pretende sublinhar é que uma definição consensual sobre o terrorismo contribui, a montante, para uma harmonização normativo-substantiva entre as diferentes ordens jurídicas nacionais e, a jusante, permite a utilização de mecanismos de cooperação judiciária internacional em matéria penal. A inexistência de tal consenso, *a contrario*, "prejudica a cooperação interestatal para trazer terroristas «à justiça»" (Ben Saul, 2021), o que pode originar situações de impunidade. Além disso, põe em cheque uma observância rigorosa do direito internacional dos direitos humanos e do direito internacional humanitário. Seja porque o princípio da legalidade criminal é posto em causa, ao nível estatal, quando o legislador nacional opta por uma definição que não é suficientemente precisa ou clara, seja porque, noutras ocasiões, a incriminação do terrorismo é de tal forma excessiva que redunda em discriminação ou limitação de liberdades políticas. Ou ainda, já no domínio do direito internacional humanitário, as consequências advenientes da incerteza de delimitação de fronteira entre terrorismo e hostilidades levadas a cabo por grupos armados não estatais.

Igualmente interessantes é o contributo de James Dorsey (2017) a propósito da crise do Golfo de 2017, com o qual enaltece aquele que, a seu ver, constitui ponto fundamental nas relações internacionais: "a ausência de uma definição consensual de terrorismo que permite aos autocratas abusar dos esforços de combate ao extremismo, reprimindo os críticos não violentos e a capacidade dos pequenos estados de traçarem o seu próprio rumo e darem socos acima do seu peso". No seu entender, esta ausência tem permitido a líderes autoritários "suprimir [em] brutalmente direitos humanos básicos, incluindo as liberdades de expressão e dos meios de comunicação social, e colocar[em] dezenas de milhares de críticos não violentos atrás das grades" (James Dorsey, 2017).

Um outro autor, Boaz Ganor, configura a definição de terrorismo como uma arma contraterrorista. Com isto quer significar que "sem uma definição de terrorismo, é impossível formular ou aplicar acordos internacionais contra o terrorismo", impossibilitando-se "a responsabilização de países que apoiam o terrorismo" ou a "tomada de passos para combater organizações terroristas e os seus aliados" (Boaz Ganor, 2002).

Igual dificuldade se descobre na delimitação e explicitação do conceito de ciberterrorismo. "Se perguntar a 10 pessoas o que é «ciberterrorismo», receberá pelo menos nove respostas diferentes!", como bem ilustram Gordon e Ford (2002).

Num importante estudo de 2015, dirigido por Lee Jarvis e Stuart Macdonald, foram questionados 118 investigadores académicos sobre as "áreas de consenso, discordância e ambiguidade nas questões conceptuais nucleares no termo ciberterrorismo" (Jarvis e Stuart Macdonald, 2015). Concluíram que, apesar da maioria estar de acordo sobre a utilidade de uma definição específica de ciberterrorismo para os responsáveis políticos e investigadores, não foi possível senão apenas uma aproximação a essa definição. Foram identificados, pela maioria dos respondentes, alguns elementos do ciberterrorismo: motivos políticos ou ideológicos, meios ou alvos digitais e a produção do medo. Mas sem um qualquer acordo sobre uma formulação exata do que seja ciberterrorismo. Neste particular, é relevante invocar as propostas de três autores: Dorothy Denning, Mark Pollitt e Barry Collin.

De acordo com Dorothy Denning (2000):

> "Ciberterrorismo é a convergência de ciberespaço e terrorismo. Refere-se aos ataques ilícitos, ou sua ameaça, dirigidos contra computadores, redes e informação aí armazenada com o propósito de intimidar ou coagir um governo ou a sua população por razões políticas ou sociais. Ademais, para ser qualificado como ciberterrorismo, um ataque deve ocasionar violência contra pessoas ou propriedade, ou pelo menos causar dano suficiente para gerar medo. Serão exemplos de ciberterrorismo os ataques que resultem em morte, ofensa à integridade física, explosões ou danos económicos severos. Ataques sérios contra infraestruturas críticas poderão ser atos de ciberterrorismo, dependendo do seu impacto. Já não o serão atos que interfiram com serviços não essenciais ou que constituam apenas um incómodo dispendioso".

Mais recentemente, em 2007, a mesma autora revisita o conceito de ciberterrorismo do seguinte modo:

> "Ciberterrorismo é um termo usualmente empregado para descrever ataques informáticos altamente lesivos ou ameaças de ataques por atores não-estatais contra sistemas de informação conduzidos para intimidar ou coagir governos ou sociedades na procura de objetivos políticos ou sociais. É a convergência de terrorismo com ciberespaço, onde o ciberespaço constitui o meio de execução do ato terrorista. Em vez de cometer atos de violência contra pessoas ou propriedade física, o ciberterrorista comete atos de destruição e disrupção contra propriedade digital. (...)

> Para ser categorizado como ciberterror, um ciberataque deve ser suficientemente destrutivo e disruptivo para gerar medo comparável ao que resulta de atos físicos de terrorismo, e deve ser praticado por motivos sociais e políticos. Ataques [contra infraestruturas críticas] (...) que causem mortes, ofensas à integridade física, falhas de energia, quedas de aviões, contaminação de água, ou perdas bancárias de milhares de milhões de dólares são exemplos" (Denning, 2007).

Já Mark Pollitt (1998) entende que "[o] ciberterrorismo é o ataque premeditado e politicamente motivado contra a informação, sistemas informáticos, programas de computador e dados que resulte em violência contra alvos civis por grupos subnacionais ou agentes clandestinos". Nos antípodas da complexidade destas definições situa-se aqueloutra de Barry Collin (autor da palavra ciberterrorismo): "a convergência entre cibernética e terrorismo" (Iqbal, 2004).

Procurando sistematizar as inúmeras aceções de ciberterrorismo, podemos reconduzi-las a uma de duas: ciberterrorismo em sentido estrito ou ciberterrorismo em sentido amplo (Jarvis e Stuart Macdonald, 2015; Brunst, 2009; O'Brien, 2021).

Genericamente reconduzem-se à primeira classe de ciberterrorismo as definições segundo as quais o ciberterrorismo corresponde a ataques politicamente motivados contra sistemas de informação dos quais resultem lesões em alvos civis. Precisamente a já referida definição de Mark Pollitt (1998) constitui um exemplo paradigmático de ciberterrorismo em sentido estrito. Do mesmo tipo de ciberterrorismo estaremos a falar mesmo quando, ainda que ao abrigo de uma nomenclatura não totalmente coincidente, se proceda a um ligeiro alargamento do seu âmbito de significado. Anna-Maria Talihärm (2010), por exemplo, refere-se a ciberterrorismo orientado para o alvo (*target-oriented cyberterrorism*), em contraposição a ciberterrorismo orientado para os meios (*tool-oriented cyberterrorism*), como "todos os ataques política ou socialmente motivados contra computadores, redes e informação, praticados por intermédio de outros computadores ou fisicamente, quando causem derramamento de sangue ou danos graves, ou medo".

De ciberterrorismo em sentido amplo estaremos a falar quando esteja em causa a utilização de meios tecnológicos por terroristas ou organizações terroristas ou, mais especificamente, o "uso da internet para propósitos terroristas" (Brunst, 2009). Neste incluem-se atividades tão diversas quanto as de recolha de fundos para utilização na prática de atos terroristas, de recrutamento, de propaganda, de comunicação, entre outras (Jarvis e Stuart Macdonald, 2015).

A opção por uma ou outra aceção de terrorismo acarreta consigo profundas diferenças no que concerne ao reconhecimento da atualidade da ameaça terrorista, definição de estratégias de prevenção e, naturalmente, de repressão do fenómeno.

Tendencialmente quem defenda uma visão mais restrita de ciberterrorismo dirá que até aos dias de hoje não se registou nenhum ato de ciberterrorismo (Clough,

2010; Sieber, 2004). A título de exemplo, Maura Conway (2014) contesta a realidade do ciberterrorismo – "[n]enhum ato de ciberterrorismo aconteceu até aos dias de hoje" –, pois para que um ato seja cunhado de ciberterrorista terá de comprovar-se a presença de motivos políticos e o uso de violência, ou pelo menos a sua ameaça. Para a autora sobressaem quatro razões explicativas da inexistência de ciberterrorismo: custo, complexidade, destruição e impacto mediático. No seu entender, a tarefa de planeamento e execução de atos ciberterroristas é bastante dispendiosa (custo) (em sentido contrário, Weimann, 2005) e demanda conhecimentos técnicos aprofundados que os membros de organizações terroristas não possuem (complexidade); o potencial de produção de danos por atos ciberterroristas é mais reduzido (destruição) e mediaticamente não são apelativos, pois não têm a mesma "teatralidade" que atos terroristas convencionais (impacto mediático).

Pelo contrário, se se assumir uma visão mais expansiva de ciberterrorismo, não sobressairá qualquer dúvida sobre a sua realidade, embora se atenue a fronteira com a mera cibercriminalidade e com isso se preste a uma confusão terminológica e conceptual. Razão essa pela qual Maura Conway (2002) rejeita tal elasticidade do conceito de ciberterrorismo. A seu ver, para que determinado ciberataque possa adquirir o epíteto de terrorista tem de ter subjacente uma motivação política e, concomitantemente, provocar medo/terror como consequência de mortes e/ou destruição em larga escala. Acaba por concluir que "[n]o que concerne à distinção entre uso terrorista de tecnologias da informação e terrorismo envolvendo tecnologia informática como arma/alvo, apenas o último pode ser definido como ciberterrorismo. O «uso» terrorista de computadores como facilitador das suas atividades, seja para propaganda, comunicações, ou outros propósitos, é apenas isso: «uso»" (Maura Conway, 2002).

Ainda que James Holt (2012) concorde que, partindo das definições mais restritas de ciberterrorismo, em particular as que integram elementos como a produção de medo ou de danos físicos, até aos dias de hoje não se assistiu a nenhum ato ciberterrorista, acrescenta igualmente que "embora não haja uma definição única acordada para o ciberterror, é claro que este termo deve encapsular uma maior gama de comportamentos do que o terror físico devido à natureza dicotómica do ciberespaço também como veículo de comunicações e como meio de ataque. Definições mais abrangentes, tais como as fornecidas pela Britz[1] e

1 "[Ciberterrorismo pode ser definido como a] a disseminação premeditada, metodológica, ideologicamente motivada de informação, facilitação da comunicação, ou, ataque contra alvos físicos, informação digital, sistemas informáticos, e/ou programas informáticos que se destinam a causar danos sociais, financeiros, físicos ou psicológicos a alvos e audiências civis com o propósito de afetar mudanças ideológicas, políticas ou sociais; ou qualquer utilização da comunicação ou informação digital que facilite tais ações direta ou indiretamente" (Britz, 2009).

Foltz[2], proporcionam um quadro muito mais abrangente para explorar as formas como os grupos extremistas utilizam a tecnologia para apoiar as suas várias agendas" (James Holt, 2012).
Assumindo uma definição mais abrangente de ciberterrorismo então a conclusão só pode ser uma: "[o] ciberterrorismo é real e constitui uma ameaça" (Foltz, 2012). Um fenómeno que pode corporizar-se nas mais diversas formas, como por exemplo a interferência ou perturbação do normal funcionamento de infraestruturas críticas, o acesso, interceção ou modificação não autorizada de dados informáticos, a desinformação, entre outras[3].

2. Porquê o Ciberespaço?

O ciberespaço enquanto expressão foi popularizado na década de 80 por William Gibson. No romance intitulado *Neuromancer*, descrevia o ciberespaço como uma "alucinação consensual experienciada diariamente por milhares de milhões de operadores legítimos, em todas as nações, por crianças a quem são ensinados conceitos matemáticos... Uma representação gráfica de dados extraídos dos bancos de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz que se estendem no não-espaço da mente, clusters e constelações de dados. Como as luzes da cidade, afastando-se" (Gibson, 1984).
Apelando a uma definição mais recente de ciberespaço, poder-se-á dizer que é um "ambiente complexo resultante da interação de pessoas, software e serviços na Internet através de dispositivos tecnológicos e redes a ela ligados, que não existe em nenhuma forma física" (ISO/IEC 27032:2012).
Alguns fatores explicam a especial adequação do ciberespaço para a prática de condutas criminosas. São eles a escala, acessibilidade, anonimato, portabilidade e transferibilidade, alcance global e ausência de guardiães capazes (Clough, 2010)[4]. No ciberespaço confluem milhares de milhões de utilizadores e dispositivos, distribuídos numa escala global, o que exponencia as oportunidades criminosas e as eleva a um patamar inédito se tivermos como referencial o contexto analógico (escala). O que se tornou possível com a democratização do acesso às novas tecno-

2 "[U]m ataque ou ameaça de ataque, motivado politicamente, destinado a: interferir com o funcionamento político, social ou económico de uma organização ou país de um grupo; induzir violência física ou uso injusto do poder; ou em conjunto com uma ação terrorista mais tradicional" (Foltz, 2012).

3 Bryan Foltz (2012) defende, no entanto, que o uso de internet como meio de planeamento ou preparação de atos terroristas – p. ex. compra de bilhetes de avião ou localização de alvos – não podem ser tidos como atos ciberterroristas.

4 Autor que é seguido de perto na explicitação dos referidos fatores.

logias (acessibilidade). A simplificação da utilização de dispositivos informáticos – p. ex. computadores, *smartphones* e *tablets* –, a diminuição dos custos de produção, distribuição e acesso aos mesmos, bem como o progressivo incremento da literacia digital contribuem significativamente para que isto acontecesse. O distanciamento espácio-temporal entre o agente do crime e a vítima e a instrumentalização da tecnologia em vista à ocultação da identidade do agente são aspetos incontornáveis desta realidade digital. Com relativa facilidade se encontram ferramentas como caixas de correio temporárias, *proxies*, redes privadas virtuais, aplicações de envio de mensagens encriptadas ou criptomoedas que, em maior ou menor medida, garantem privacidade e anonimato (Weimann, 2005) aos seus utilizadores (anonimato). A portabilidade e transferibilidade referem-se, por sua vez, à miniaturização dos dispositivos informáticos e à evolução avassaladora da sua capacidade de processamento, transmissão e alojamento de dados informáticos. Indubitavelmente se torna mais simples o planeamento e execução de condutas criminosas com o advento de sistemas de informação verdadeiramente móveis como, por exemplo, os *smartphones* (portabilidade e transferibilidade). A exploração do ciberespaço com um propósito criminoso aproveita a fluidez geográfica do mesmo. Ocorre uma autêntica desconstrução do entendimento tradicional das noções de espaço e tempo, na exata medida em que o distanciamento físico e o investimento temporal necessário para o suprir perdem todo o seu sentido. De um ponto de vista tecnológico-comunicacional é praticamente indiferente o local onde o agente e vítima se encontram (Weimann, 2005). Basta uma conexão à internet (alcance global). O que se traduz numa enorme dificuldade prática no desenvolvimento de investigações criminais eficazes e na articulação entre autoridades judiciárias e policiais dos vários países envolvidos, cujas ordens jurídicas se regem por paradigmas clássicos de territorialidade e soberania nacional em matéria de exercício da ação penal. Quanto a este aspeto é esclarecedor Jonathan Clough (2010) ao afirmar que "[t]al como no ambiente offline, não é prático nem desejável que a polícia esteja em todo o lado. O papel de «guardião» deve ser partilhado com outros em toda a comunidade, quer se trate de pais que monitorizam a utilização da Internet pelos seus filhos, de instituições financeiras que procuram transações suspeitas ou de administradores de sistemas que detetam intrusões na rede. Todos desempenham um importante papel de tutela, tal como os grupos industriais e os reguladores governamentais. Os ISP são particularmente significativos, sendo efetivamente os guardiões dos dados na Internet".

3. Ciberterrorismo no Contexto da Lei de Combate ao Terrorismo

Dando cumprimento à Decisão-Quadro 2002/475/JAI do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo, foi aprovada no nosso ordenamento

jurídico a Lei n.º 52/2003[5]. Apesar das sucessivas alterações que foi sofrendo – sendo a mais recente aquela que decorreu da Lei n.º 79/2021 –, o seu objeto manteve-se desde o seu início: a previsão e punição de atos e organizações terroristas.

Mais rigorosamente, o legislador português prevê a incriminação das organizações terroristas (Artigo 2.º e 3.º), dos atos terroristas em sentido próprio (Artigo 4.º, n.º 1 e 2), incitamento público à prática de atos terroristas (Artigo 4.º, n.º 3 e 4), acesso a mensagens de incitamento público à prática de atos terroristas com propósito de recrutamento (Artigo 4.º, n.º 5), recrutamento para a prática de atos terroristas (Artigo 4.º, n.º 6), treino para a prática de atos terroristas (Artigo 4.º, n.º 7), apologia pública da prática de atos terroristas (Artigo 4.º, n.º 8 e 9), viagem de treino para a prática de atos terroristas (Artigo 4.º, n.º 10), viagem para a prática de atos terroristas ou adesão a organizações terroristas (Artigo 4.º, n.º 11), apoio a viagem para a prática de atos terroristas ou adesão a organizações terroristas (Artigo 4.º, n.º 12), terrorismo internacional (Artigo 5.º) e financiamento do terrorismo (Artigo 5.º-A).

Numa leitura mais atenta dos Artigos 2.º e 3.º ressalta imediatamente o facto de não haver qualquer referência a motivações religiosas, políticas ou ideológicas (Ganor, 2001). Conjugando as referidas normas retira-se a seguinte definição de terrorismo: prática de um ato contra a vida, a integridade física ou liberdade das pessoas, contra a segurança dos transportes e das comunicações, de produção dolosa de perigo comum, de perturbação grave ou distribuição de infraestruturas críticas, de investigação e desenvolvimento de armas biológicas ou químicas, ou de emprego de energia nuclear, armas de fogo, biológicas ou químicas, substâncias ou engenhos explosivos, meios incendiários de qualquer natureza, encomendas ou cartas armadilhadas, com o propósito de prejudicar a integridade e a independência nacionais, impedir, alterar ou subverter o funcionamento das instituições do Estado previstas na Constituição, forçar a autoridade pública a praticar um ato, a abster-se de o praticar ou a tolerar que se pratique, ou ainda intimidar certas pessoas, grupos de pessoas ou a população em geral, desde que a conduta do agente seja suscetível de afetar gravemente o Estado ou a população que vise intimidar[6].

5 Sobre a transposição desta Decisão-Quadro, cf. Dias e Caeiro (2005). A lei de combate ao terrorismo (Lei n.º 52/2003, de 22 de agosto): sobre a transposição para o direito português, da decisão-quadro do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo. *Revista de Legislação e de Jurisprudência*, 135(3935), pp.70-89.

6 Para uma análise do tipo subjetivo de ilícito, Fernandes, C., 2010. Lei n.º 52/2003, de 22 de agosto. In: P. Albuquerque e J. Branco, coord., *Comentário das Leis Penais Extravagantes*. Lisboa: Universidade Católica Editora, pp. 212-213; Sousa, S., Godinho, I. e Machado, P., 2022. Artigo 2.º – organizações terroristas. In: J. Linhares e M. Antunes, coord., *Terrorismo: legislação comentada: textos doutrinais*. Coimbra: Imprensa da Universidade de Coimbra, pp. 27-29 e 37.

Em bom rigor, o legislador português segue a liderança da União Europeia[7]. No considerando 3 da Decisão-Quadro 2002/475/JAI do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo, lê-se que "[o] conjunto dos Estados-Membros, ou alguns deles, são parte num certo número de convenções em matéria de terrorismo. A Convenção do Conselho da Europa, de 27 de Janeiro de 1977, para a repressão do terrorismo, não considera as infrações terroristas infrações políticas ou conexas, nem inspiradas por móbeis políticos". E, adiante, no Artigo 1.º, na densificação do conceito de infração terrorista, não vislumbra menção alguma à necessidade de verificação de motivações políticas, ideológicas ou religiosas. Nos termos do n.º 1 desse artigo, o objetivo da prática dos atos aí referidos há de enquadrar-se num dos três seguintes, para que se possa falar de ato terrorista: intimidação grave de uma população; coação indevida dos poderes públicos ou uma organização internacional à prática de um ato ou à sua abstenção; desestabilização grave ou destruição de estruturas fundamentais políticas, constitucionais, económicas ou sociais de um país ou de uma organização internacional[8].
Não se pode por isso afirmar que no Artigo 1.º da Decisão-Quadro e nos Artigos 2.º e 3.º da Lei n.º 52/2003 se exija, no quadro da incriminação típica, a presença dos elementos subjetivos habitualmente apontados aos autores de atos terroristas. Conforme nos dá conta Thomas Weigend (2006),

> "[o]s terroristas têm normalmente um triplo objetivo: têm a intenção "normal" de cometer o crime básico de homicídio, bombardeamento, agressão, etc.; pretendem, além disso, intimidar um grupo ou a população em geral e/ou obrigar outros a praticar atos (por exemplo, libertar prisioneiros políticos); e têm motivos políticos ou ideológicos ulteriores, por exemplo, para desestabilizar o atual governo ou para derrotar uma religião ou ideologia rivais. Os instrumentos legais diferem quanto à medida em que requerem todos ou apenas alguns destes elementos subjetivos ideais-tipo para uma condenação por terrorismo".

Radicará na rejeição como elemento típico da motivação política (ou outra) a ideia de que constituiria um fator de maior complexidade ou confusão. Exatamente neste sentido se pronunciou Kalliopi K. Koufa (2003), Relatora Especial das Nações

7 No âmbito do Conselho da Europa, é relevante a Convenção Europeia para a Repressão do Terrorismo, de 1977. O Artigo 1.º da Convenção consagra a regra de que, para efeitos de extradição, os crimes aí previstos não serão considerados crimes políticos ou politicamente motivados, ou crimes conexos a crimes políticos. A razão para esta opção é simples: a categorização de um ato terrorista como crime político ou politicamente motivado impossibilitaria a extradição do seu autor (Conselho da Europa, 1977). Cf. Artigo 3.º da Convenção Europeia de Extradição.

8 O mesmo consta da Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo, que substituiu a Decisão-Quadro 2002/475/JAI do Conselho.

Unidas para o terrorismo e direitos humanos, num relatório preparado no contexto das Nações Unidas (E/CN.4/Sub.2/2003/WP.1):

> "[e]m qualquer caso, embora as categorias amplas ou gerais dificilmente possam alcançar precisão e fazer plena justiça à variedade e complexidade dos fenómenos terroristas, tentativas de conceber subdivisões e distinções analíticas e mais sofisticadas que forneçam delimitações mais precisas ou informações sobre subgrupos de terrorismo – tais como a sua estrutura organizacional, tamanho, potencial relações com Estados e graus dessas relações, a sua identidade, características, motivações sociais, políticas, culturais e psicológicas, etc. – são demasiado complicadas e diversificadas e, acima de tudo, servem apenas as necessidades do utilizador particular. Por muito úteis que sejam para iluminar aspetos particulares dos fenómenos do terrorismo e dos terroristas, e para contribuir para a nossa compreensão da natureza abrangente da problemática que os rodeia, são de pouca utilidade para identificar exatamente o que constitui terrorismo e quem são os terroristas".

Há ainda quem entenda que, além desta camada de complexidade que resultaria para a tarefa de investigação e julgamento, sobretudo quando as motivações por detrás de um ato terrorista não são claras, evidentes ou manifestas, a não inclusão dos motivos políticos, ideológicos ou religiosos permite o evitamento da explicitação do sentido e alcance dessas palavras (política, ideologia e religião), além de permitir uma maior compatibilidade dogmática com as ordens jurídico-penais onde os motivos não são elemento típico relevante (Borgers, 2012).

O resultado desta opção é claro: a interpretação do conceito de terrorismo à luz dos referidos instrumentos jurídicos dispensa a comprovação de um motivo político, ideológico ou religioso enquanto elemento subjetivo adicional, apesar de estes serem tidos pela doutrina dominante como características fundamentais do terrorismo (Borgers, 2012; Dumitriu, 2004; Thomas Weigend, 2006). O que leva a um alargamento da matéria proibida e ao enquadramento como terrorismo de atos que, seguindo-se a indicação da generalidade da doutrina internacional, verdadeiramente não o são[9] (Borgers, 2012).

Colocando de parte este debate em torno da correção da definição de terrorismo e apontando a nossa atenção para a questão de saber se afinal o ciberterrorismo encontra amparo na lei portuguesa, a resposta é afirmativa.

Por um lado, se recensearmos os crimes comuns referidos nas várias alíneas do Artigo 2.º, n.º 1, não será descabido conjeturar a punição do ciberterrorismo, mesmo

9 Veja-se o caso do ataque à Academia de Alcochete. Relevante neste domínio, Brandão, N., 2020. O caso do ataque à Academia de Alcochete sob a perspetiva do crime de terrorismo. Anotação ao acórdão do Juízo Central Criminal de Almada (Juiz 3) de 28 de maio de 2020. *Revista Portuguesa de Ciência Criminal*, 30, pp.403-430.

na sua aceção mais restrita. Barry Collin (1996) avança com algumas hipóteses que nos poderão ser úteis: "acesso remoto aos sistemas de controlo de processamento de um fabricante de cereais, [alteração dos] níveis de suplemento de ferro, e [causação da morte de] crianças (...) que os ingiram"; "[ataque à] próxima geração de sistemas de controlo de tráfego aéreo, [fazendo colidir] duas grandes aeronaves civis"; "[alteração remota de] fórmulas de medicamentos nos fabricantes farmacêuticos. A potencial perda de vidas é insondável"; [alteração remota de] pressão nas linhas de gás, causando uma falha de válvula, e um bloco de um subúrbio adormecido detona e queima".

Genericamente qualquer um dos crimes-base cujo *iter criminis* não esteja descrito tipicamente poderá constituir uma situação de ciberterrorismo em sentido estrito desde que se trate um ato violento para com alvos civis, com intenção terrorista, e a sua execução se der por intermédio do ciberespaço (Pollitt, 1998).

Se o nosso referencial teórico for, antes, o do ciberterrorismo em sentido amplo, *i. e.*, de classificação como ato terrorista o "uso da internet para propósitos terroristas" (Brunst, 2009), são múltiplas as hipóteses previstas na Lei n.º 52/2003. Exemplificativamente temos o incitamento público à prática de atos terroristas, por meio de comunicação eletrónica, com difusão de mensagens acessíveis por internet (Artigo 4.º, n.º 4), acesso através de sistema informático a mensagens de incitamento público à prática de atos terroristas com propósito de recrutamento (Artigo 4.º, n.º 5), apologia por meio de comunicação eletrónica, acessível por Internet, da prática de atos terroristas (Artigo 4.º, n.º 9).

Conclusão

O conceito de terrorismo e, inerentemente, de ciberterrorismo é amplamente discutido na esfera internacional há décadas, sem que se tenha obtido um resultado merecedor de consenso. Embora não tenha impedido a normatização de estratégias de prevenção e repressão do terrorismo – e do seu financiamento –, quer numa dimensão nacional quer internacional, a descrição típica do que seja terrorismo, presente nesses instrumentos jurídicos, é objeto de fundadas dúvidas quanto ao seu sentido e alcance, precisamente devido ao seu carácter poliédrico e controverso.

O aproveitamento do ciberespaço como um novo palco do fenómeno do terrorismo – nos seus múltiplos desdobramentos: financiamento, propaganda e apologia, recrutamento, planeamento e execução – é, em certa medida, expectável e explicável pela escala, acessibilidade, anonimato, portabilidade e transferibilidade, alcance global e ausência de guardiães capazes (Clough, 2010). Surge então o ciberterrorismo, noção essa tão ou mais discutida do que aquela que lhe dá origem, desde logo porque certa doutrina contesta a sua realidade prática. Adeptos de uma noção

mais estrita do ciberterrorismo, situam este fenómeno numa dimensão meramente teórica ou académica, na medida em que, no seu entender, não se registou até hoje um ataque politicamente motivado contra sistemas de informação do qual haja resultado vítimas civis. No outro lado do espectro populam propostas definitórias, de diferentes colorações, que reconhecem no ciberterrorismo um fenómeno mais abrangente onde a utilização de ferramentas digitais assume um papel de maior destaque na concretização dos seus elementos constitutivos.

Ao voltarmos a nossa atenção para a lei portuguesa de luta contra o terrorismo – Lei n.º 52/2003 – não se descobre uma qualquer referência a esta disputa de pendor marcadamente doutrinal. No entanto, uma leitura atenta das normas aí previstas permite concluir que não se pune somente o fenómeno do terrorismo na sua aceção tradicional, mas também o ciberterrorismo, em ambas as dimensões.

Bibliografia

Bell, J., 1978. *A time of terror*: *How Democratic Societies Respond to Violence*. Nova Iorque: Basic Books.

Borgers, M., 2012. Framework Decision on Combating Terrorism: Two Questions on the Definition of Terrorist Offences. *New Journal of European Criminal Law*, 3(1), pp.68-82.

Brandão, N., 2020. O caso do ataque à Academia de Alcochete sob a perspectiva do crime de terrorismo. Anotação ao acórdão do Juízo Central Criminal de Almada (Juiz 3) de 28 de Maio de 2020. *Revista Portuguesa de Ciência Criminal*, 30, pp. 403-430.

Britz, M., 2009. *Computer forensics and cyber crime*. 2.ª ed. Upper Saddle River: Prentice-Hall.

Brunst, P., 2010. Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In: M. Wade e A. Maljevic, ed., *A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications*. Nova Iorque: Springer, pp. 51-78.

Bryan Foltz, C., 2004. Cyberterrorism, computer crime, and reality. *Information Management & Computer Security*, 12(2), pp.154-166.

Clough, J., 2010. *Principles of cybercrime*. 1.ª ed. Cambridge: Cambridge University Press.

Collin, B., 1996. *The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge*.

Conselho da Europa, 1977. *Relatório explicativo da Convenção Europeia para a Repressão do Terrorismo.*

Conway, M., 2002. Reality bytes: cyberterrorism and terrorist 'use' of the Internet. *First Monday*, 7(11).

Conway, M., 2014. Reality Check: Assessing the (Un)Likelihood of Cyberterrorism. In: T. Chen, L. Jarvis e S. Macdonald, ed., *Cyberterrorism*. Nova Iorque: Springer, pp. 103-121.

Denning, D., 2006. A View of Cyberterrorism Five Years Later. In: K. Himma, ed., *Internet Security: Hacking, Counterhacking, and Society*. Londres: Jones and Bartlett Publishers, pp.123-140.

Denning, D., 2000. *Cyberterrorism Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives.* 23 de maio. Disponível em http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Dias, F. e Caeiro, P., 2005. A lei de combate ao terrorismo (Lei n.º 52/2003, de 22 de Agosto): sobre a transposição para o direito português, da decisão-quadro do Conselho, de 13 de Junho de 2002, relativa à luta contra o terrorismo. *Revista de Legislação e de Jurisprudência.* 135(3935), pp. 70-89.

Dorsey, J., 2017. The Gulf Crisis: Grappling for a face saving solution. *South Asia Journal*, June 19. Disponível em http://southasiajournal.net/the-gulf-crisis-grappling-for-a-face-saving-solution/ [acedido em 5 de março de 2022].

Dumitriu, E., 2004. The E.U.'s Definition of Terrorism: The Council Framework Decision on Combating Terrorism. *German Law Journal*, 5(5), pp. 585-602.

Ganor, B., 2002. Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? *Police Practice and Research*, 3(4), pp. 287-304.

Fernandes, C., 2010. Lei n.º 52/2003, de 22 de Agosto. In: P. Albuquerque e J. Branco, coord., *Comentário das Leis Penais Extravagantes*. Lisboa: Universidade Católica Editora, pp. 193-232.

Ganor, B., 2001. Terrorism: No Prohibition Without Definition. *ICT* [em linha], 7 de novembro. International Institute for Counter-Terrorism. Disponível em https://www.ict.org.il/Article.aspx?ID=1588#gsc.tab=0

Gibson, W., 1984. *Neuromancer*. Nova Iorque: Penguin Group.

Gordon, S. e Ford, R., 2002. Cyberterrorism? *Computers and Security*, 21(7), pp. 636-647.

Hoffman, B., 2006. *Inside Terrorism*. Nova Iorque: Columbia University Press.

Holt, T., 2012. Exploring the Intersections of Technology, Crime, and Terror. *Terrorism and Political Violence*, 24(2), pp. 337-354.

Iqbal, M., 2022. Defining Cyberterrorism. *Journal of Computer & Information Law*, 22(2), pp. 397-408.

ISO, 2012. *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity*. 1st ed. [pdf]. Disponível em https://www.iso.org/standard/44375.html [acedido em 1 de abril de 2022].

Jarvis, L. e Macdonald, S., 2014. What Is Cyberterrorism? Findings From a Survey of Researchers. *Terrorism and Political Violence*, 27(4), pp. 657-678.

Jenkins, B., 2004. Semantics are Strategic in the War on Terror. *The RAND Blog*, September 30. Disponível em https://www.rand.org/blog/2004/09/semantics-are-strategic-in-the-war-on-terror.html [acedido em 31 de março de 2022].

Koufa, K., 2003. *Specific human rights issues: new priorities, in particular terrorism: additional progress report*. Geneva: Nações Unidas.

Laqueur, W., 2007. Terrorism: A Brief History. *US Department of State e-Journal*, Disponível em https://www.hsdl.org/?view&did=474007/ [acedido 31 março 2022].

Laqueur, W., 1987. *The age of terrorism*. Londres: Weidenfeld and Nicolson.

Marsili, M., 2018. The War on Cyberterrorism. *Democracy and Security*, 15(2), pp. 172-199.

Martin, G., 2011. *Essentials of terrorism: Concepts and Controversies*. 2.ª ed. Thousand Oaks: Sage Publishing.

Matusitz, J., 2005. Cyberterrorism: How Can American Foreign Policy Be Strengthened in the Information Age? *American Foreign Policy Interests*, 27(2), pp. 137-147.

O'Brien, C., 2021. What is cyber-terrorism, and is it a threat to U.S. national security? *Small Wars Journal*, às 2:32 am, de 11 de abril. Disponível em https://smallwarsjournal.com/jrnl/art/what-cyber-terrorism-and-it-threat-us-national-security

Pollitt, M., 1998. Cyberterrorism – fact or fancy? *Computer Fraud & Security*, 1998(2), pp. 8-10.

Saul, B., 2021. The Legal Black Hole in United Nations Counterterrorism. *Global Observatory*, June 2, International Peace Institute. Disponível em https://theglobalobservatory.org/2021/06/the-legal-black-hole-in-united-nations-counterterrorism/ [acedido em 31 de março de 2022].

Schmid, A., 2020. Revisiting the Wicked Problem of Defining Terrorism. In: G. Brunton e T. Wilson, ed., Terrorism: Its Past, Present & Future Study – A Special Issue to Commemorate CSTPV at 25. *Contemporary Voices: St Andrews Journal of International Relations*, 1(4), pp. 3-11.

Schmid, A., 2004. Terrorism – The Definitional Problem. *Case Western Reserve Journal of International Law*, 36(2), pp. 375-419.

Schmid, A., 2011. *The Routledge Handbook of Terrorism Research*. Londres: Routledge.

Schmid, A. e Jongman, A., 2005. *Political terrorism*. New Brunswick: Transaction Publishers.

Sieber, U., 2022. The Threat of Cybercrime. In: Conselho da Europa, ed., *Organized Crime in Europe: The Threat of Cybercrime*. Estrasburgo: Conselho da Europa, pp. 81-217.

Sousa, S., Godinho, I. e Machado, P., 2022. Artigo 2.º – Organizações Terroristas. In: J. Linhares e M. Antunes, coord., *Terrorismo: legislação comentada – textos doutrinais*. Coimbra: Imprensa da Universidade de Coimbra, pp. 23-42.

Talihärm, A., 2020. Cyberterrorism: in Theory or in Practice? *Defence Against Terrorism Review*, 3(2), pp. 59-74.

Weigend, T., 2006. The Universal Terrorist: The International Community Grappling with a Definition. *Journal of International Criminal Justice*, 4(5), pp. 912-932.

Weimann, G., 2005. Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism*, 28(2), pp. 129-149.