INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

VI CURSO DE COMANDO E DIREÇÃO POLICIAL

Trabalho Individual Final

A Radicalização *Online* e o Terrorismo Jihadista: Desafios para a Segurança Interna

Estudo teórico

Auditor/a

André Daniel Ferreira Teixeira

Lisboa, 10 de outubro de 2025

"(…) a perceção de controlo, por parte dos indivíduos, cede à certeza de que a incerteza não é dominável."

(Fiães Fernandes, 2014, p. 21)

RESUMO

A radicalização *online* tem-se afirmado como um dos principais vetores de mobilização ideológica para o terrorismo jihadista, explorando as dinâmicas do ciberespaço para disseminar a propaganda, recrutar novos seguidores e incitar à violência. Este fenómeno, de natureza transnacional, desafia os modelos tradicionais da segurança e exige uma abordagem multidisciplinar que articule as dimensões tecnológicas, sociopolíticas e jurídicas.

Este estudo foca-se na influência das tecnologias de informação e comunicação, para as dinâmicas contemporâneas do terrorismo, fazendo emergir novos desafios para a segurança interna. De natureza teórica, o trabalho traça um olhar pela transição de modelos tradicionais de radicalização para os ecossistemas digitais. O estudo demonstra que a *internet* não é apenas um meio de difusão de propaganda, mas um espaço de pertença e socialização ideológica que acelera e amplia o processo de radicalização. Conclui-se que o combate a este fenómeno requer uma abordagem multidimensional que una a inovação tecnológica, a cooperação interinstitucional e o reforço da resiliência social e democrática como pilares da segurança interna.

Palavras-chave: prevenção, radicalização *online*; segurança interna; terrorismo jihadista.

ABSTRACT

Online radicalisation has emerged as one of the principal vectors of ideological mobilisation in jihadist terrorism, exploiting the dynamics of cyberspace to disseminate propaganda, recruit new followers, and incite violence. This transnational phenomenon challenges traditional security models and necessitates a multidisciplinary approach that integrates technological, socio-political, and legal dimensions.

This study examines the influence of information and communication technologies on contemporary terrorism dynamics, highlighting the new challenges posed to internal security. It also demonstrates that the internet serves not only as a way for spreading propaganda but also as a space for belonging and ideological socialisation, which accelerates and amplifies the radicalisation process. Furthermore, this work explores the transition from traditional radicalisation models to digital ecosystems. It concludes that combating this phenomenon requires a multidimensional strategy that combines technological innovation, inter-institutional cooperation, and the strengthening of social and democratic resilience as foundational pillars of internal security.

Keywords: internal security; jihadist terrorismo; online radicalisation; prevention.

ÍNDICE

1. INTRODUÇÃO

O fenómeno da radicalização jihadista constitui um dos principais desafios à segurança europeia do século XXI. A sua evolução reflete uma transformação profunda na natureza das ameaças, marcada pela descentralização das redes terroristas, pela mobilização de atores solitários e, sobretudo, pela crescente utilização das tecnologias digitais como meio de difusão ideológica e de recrutamento. A digitalização do extremismo tem vindo a alterar as dinâmicas tradicionais do terrorismo, permitindo que a radicalização se desenvolva de forma difusa, transnacional e muitas vezes invisível aos mecanismos clássicos de controlo e vigilância.

Apesar da evolução das políticas de segurança, o terrorismo continua a manifestar-se de forma imprevisível, explorando vulnerabilidades legais e tecnológicas. O contexto digital abriu novas possibilidades para a disseminação de ideologias extremistas, facilitando a mobilização e o recrutamento à distância, ultrapassando as fronteiras tradicionais, o que acarreta novos desafios para a segurança (Ventura & Carvalho, 2020). Este contexto digital comporta múltiplas dimensões, podendo até ser considerado uma "arma psicológica numa infoguerra global, capaz de moldar comportamentos e ameaçar a autodeterminação individual" (Fernandes, 2025, p. 33).

A União Europeia (UE) reconhecendo esta mutação, procura reforçar o seu quadro normativo e operacional no combate à difusão de conteúdos extremistas *online*. Em simultâneo, os Estados-Membros enfrentam o desafio de adaptar os seus sistemas nacionais de segurança interna às ameaças emergentes, que se manifestam tanto no ciberespaço como no espaço físico.

Com inspiração nos vetores de ameaça identificados no *European Union Terrorism Situation and Trend Report* (Europol, 2025a), o presente estudo comporta uma temática atual e relevante para o desenvolvimento das ciências policiais e da segurança interna, procurando contribuir com uma análise crítica suportada na literatura especializada.

A reflexão sobre os desafios que se colocam à segurança interna europeia e nacional pode assumir uma dimensão estratégica e prospetiva, apontando para a necessidade de reforçar a coordenação interinstitucional, a literacia digital e a resiliência social como pilares de uma abordagem integrada à prevenção do extremismo violento.

O trabalho estrutura-se em torno de duas questões fundamentais: (a) de que modo a radicalização *online* tem influenciado as dinâmicas terroristas? e (b) quais são os desafios para a segurança interna?

Para responder a estas questões, estabeleceram-se dois objetivos principais: (i) compreender os processos de radicalização contemporânea mediados pelas tecnologias de informação e comunicação; e (ii) identificar os desafios que se colocam à segurança interna.

A organização do trabalho estrutura-se em dois capítulos principais: o estado da (evolução do jihadismo, as estratégias de propaganda digital e os processos de radicalização) e as perspetivas (quadro europeu e nacional de resposta, com especial enfoque nas políticas de prevenção e nos desafios para a segurança interna).

1.1 Método

O presente estudo segue uma abordagem de natureza teórica e qualitativa, centrada na revisão da literatura especializada sobre radicalização jihadista e a segurança interna. O percurso metodológico foi delineado de forma a garantir a coerência entre o problema de partida, as questões de investigação e os objetivos definidos, em conformidade com os princípios metodológicos enunciados por Quivy e Van Campenhoudt (2005), segundo os quais a articulação entre o problema, as questões e o método constitui o eixo estruturante de toda a investigação científica. Assim, partindo da identificação do problema, a influência da radicalização online nas dinâmicas terroristas e os desafios daí decorrentes para a segurança interna, foram formuladas as questões de partida e delineados os objetivos correspondentes, orientando a seleção das fontes e a organização da análise.

A metodologia adotada privilegiou a análise documental e comparativa, com vista à construção de uma síntese crítica e fundamentada sobre o estado de arte e as perspetivas de resposta institucional.

2. ESTADO DE ARTE

2.1 Evolução do terrorismo jihadista

O conceito terrorismo jihadista "é usado para nomear uma variante do terrorismo internacional que se baseia numa interpretação extremista, e violenta, do Islão para fomentar os seus objectivos político-ideológicos." (Matos, 2016, p. 256).

O terrorismo jihadista tem sofrido transformações significativas desde o seu surgimento como força organizada no final do século XX. Inicialmente associado à luta contra a ocupação soviética no Afeganistão, o movimento jihadista ganhou projeção internacional com a fundação da *Al-Qaeda* por Osama Bin Laden, que viria a protagonizar os atentados de 11 de setembro de 2001. Este evento marcou uma viragem estratégica e simbólica, projetando o jihadismo como uma ameaça transnacional e inaugurando a chamada guerra global ao terrorismo (Duarte, 2015).

A estrutura descentralizada seguida pela *Al-Qaeda* permitiu a criação de filiais regionais, entre elas a *Al-Qaeda* no Iraque, liderada por Abu Musab al-Zarqawi. Esta filial destacou-se pela brutalidade dos ataques e pela forte componente sectária contra xiitas, o que gerou tensões com a liderança central da *Al-Qaeda*. Após a morte de al-Zarqawi em 2006, o grupo passou a designar-se por Estado Islâmico do Iraque, conhecido internacionalmente através do acrónimo (ISI), iniciando um processo de autonomização ideológica e operacional que, mais tarde culminou na segregação com a *Al-Qaeda* (Rato, 2016).

Em 2013, o grupo adotou o nome Estado Islâmico do Iraque e do Levante, conhecido internacionalmente através do acrónimo (ISIS), e em 2014 proclamou o califado, assumindo definitivamente a designação de Estado Islâmico, também conhecido internacionalmente como *Daesh*. Esta transformação representou não apenas uma mudança de nome, mas uma redefinição estratégica. Enquanto a *Al-Qaeda* apontava para o califado como um objetivo secundário, o Estado Islâmico procurou instaurá-lo de imediato, com controlo efetivo de territórios e das populações. A divergência entre os dois grupos foi-se acentuando, ao ponto de Estado Islâmico acusar a *Al-Qaeda* de moderação excessiva e a *Al-Qaeda* criticar o Estado Islâmico pela sua brutalidade e falta de visão estratégica (Cockburn, 2014; Arena, 2022).

Esta concorrência acabou por fomentar novas estratégias e abordagens de hostilizar o Ocidente, levando consigo a transformação do jihadismo através da transição de organizações centralizadas para estruturas em rede, com células autónomas e capacidade de

atuação independente. Como destaca John Gray (2003), a *Al-Qaeda* é uma organização moderna, comparável a uma multinacional descentralizada, que utiliza tecnologias como satélites, redes encriptadas e redes sociais para disseminar a sua mensagem e coordenar as ações.

É neste contexto que a radicalização jihadista passou a marcar presença mais assídua no continente europeu, através de processos de *homegrown radicalisation*, envolvendo jovens imigrantes de segunda e terceira geração (Europol, 2025a; Soares, 2013-2014-2015).

O jihadismo global não é apenas uma manifestação violenta do Islão, mas sim uma estratégia racional e instrumental, com objetivos políticos bem definidos. A sua capacidade de adaptação às contingências geopolíticas tem garantido a sobrevivência da ideologia jihadista, mesmo após perdas territoriais significativas (Duarte, 2015).

A radicalização digital tornou-se assim um vetor essencial na expansão do jihadismo. As plataformas de redes sociais são hoje utilizadas para disseminar doutrinas extremistas, glorificar o martírio e promover a *jihad* como forma de resistência contra o Ocidente.

Em linha com a literatura revista, considera-se que as organizações terroristas utilizam a *internet* de forma estratégica para diversos fins essenciais, nomeadamente: coordenação e planeamento de ações, treino de militantes, financiamento, propaganda e mobilização de novos membros. Estas organizações recorrem às novas plataformas digitais para promover a radicalização e o recrutamento de apoiantes em diferentes partes do mundo, utilizando a propaganda como ferramenta de sedução e mobilização (Davis, 2006; Shultz, 2008; Weimann, 2014; U.S. S. Committee, Homeland Security, Gov. Affairs, 2015; Duarte, 2015; Arena, 2022; Kaczkowski, et al., 2021; Matos, 2016).

2.2 Estratégias de propaganda digital do Estado Islâmico

A propaganda digital do Estado Islâmico constitui uma das mais sofisticadas ferramentas de radicalização e mobilização no terrorismo jihadista contemporâneo. Tal como evidenciado anteriormente, desde a sua ascensão em 2014, o Estado Islâmico demonstrou uma capacidade notável de adaptação às plataformas digitais, utilizando-as para disseminar narrativas ideológicas, recrutar combatentes e legitimar a sua pretensão de califado global.

O autor Nuno Lemos Pires sublinha que a "força das ideologias e religiões é muito mais forte quando o quadro de referência onde se vive se deteriora e não representa quem o habita" (2016, p. 59), o que contribui para a adesão a narrativas extremistas em contextos de desagregação social e política. Esta leitura reforça a ideia de que a propaganda jihadista não

depende apenas de recursos técnicos, mas também de condições socioculturais que favorecem a radicalização.

O Estado Islâmico construiu uma narrativa visual e textual que transcende fronteiras, combinando elementos religiosos, políticos e emocionais para criar uma identidade jihadista global (Kaczkowski, et al., 2021). Esta narrativa é disseminada através de vídeos de alta qualidade, revistas digitais como a *Dabiq* e a *Rumiyah*, e uma presença ativa nas redes sociais, bem como nas aplicações encriptadas.

O estudo de Kaczkowski et al. revela que existe uma relação direta entre o controlo territorial do Estado Islâmico e a produção da propaganda virtual. Os autores referem que, durante os períodos de expansão territorial, o grupo aumentou a produção de imagens militares e de recrutamento, no entanto, à medida que foram perdendo território, "a campanha mediática do ISIS deslocou o foco visual das revistas e boletins informativos, de imagens militares para imagens de construção estatal (…)" (2021, p. 11), numa tentativa de reafirmar a legitimidade do califado e manter a moral dos apoiantes. Aliás, considera-se mesmo que esta mudança estratégica, reflete uma tentativa de sustentar a perceção de continuidade governativa, mesmo perante derrotas militares.

A segmentação das audiências é outro elemento central da estratégia comunicacional do Estado Islâmico. As revistas *Dabiq* e *Rumiyah*, dirigidas a públicos não árabes e editadas com dez idiomas, procuravam recrutar estrangeiros e incitar ataques no Ocidente, enquanto o boletim *al-Naba'*, editado em árabe, visava essencialmente convencer as populações locais da viabilidade do projeto estatal jihadista (Kaczkowski et al., 2021). Esta diferenciação linguística e temática demonstra uma compreensão profunda dos públicos-alvo e das suas motivações.

Por outro lado, esta dinâmica descentralizada dificulta a ação das autoridades, uma vez que o conteúdo não depende exclusivamente dos canais oficiais, circulando por diferentes vias de comunicação em simultâneo, tais como fóruns, redes sociais e plataformas de partilha encriptadas (Conway, 2017).

A sofisticação da propaganda do Estado Islâmico reside também na sua capacidade de explorar os algoritmos das plataformas digitais. A este respeito, o artigo de Awan sobre o ciberextremismo, analisa o uso das redes sociais como ferramenta de propaganda digital, recrutamento e radicalização pelo Estado Islâmico. A investigação baseou-se na análise de 100 páginas do *Facebook* e 50 contas do *Twitter*, utilizando o software *NVivo* para identificar padrões discursivos e comportamentais. Segundo o autor, "a internet tornou-se uma

ferramenta poderosa para grupos terroristas, permitindo-lhes alcançar audiências globais com facilidade" (Awan, 2017, p. 138).

O autor recorreu a uma tipologia composta por sete perfis de comportamento *online* associados à radicalização: *cyber mobs*, *loners*, *fantasists*, *thrill seekers*, *moral crusaders*, *narcissists* e *identity seekers*. Esta categorização permitiu compreender as motivações psicológicas e sociais que sustentam o envolvimento com conteúdos extremistas. Por exemplo, os *thrill seekers* são atraídos pela violência e adrenalina, enquanto os *identity seekers* procuram o sentido de pertença (Awan, 2017). Adicionalmente, o autor destaca que o Estado Islâmico emprega estratégias sofisticadas de comunicação digital, incluindo vídeos virais, *hashtags* e aplicações móveis, para amplificar a sua mensagem.

Outro vetor da propaganda do Estado Islâmico é visível na mobilização de combatentes estrangeiros e na inspiração de ataques terroristas em solo europeu. Neste âmbito, Neumann (2016) argumenta que a radicalização *online* funciona como uma espécie de catalisador ideológico, acelerando processos que, em contextos *offline*, seriam mais lentos. Esta aceleração representa um desafio crítico para os serviços de segurança interna, acarretando dificuldades em detetar, precocemente, os sinais de radicalização digital.

A resposta das autoridades europeias tem revelado alguma consistência nas políticas de combate ao terrorismo, procurando acompanhar as dinâmicas que estes grupos têm adotado. A este respeito, destaca-se o Regulamento da União Europeia 2021/784, do Parlamento Europeu e do Conselho, de 29 de abril de 2021, relativo ao combate à difusão de conteúdos terroristas em linha.

No entanto, Bartlett e Miller (2011) alertam que a eficácia das contra narrativas depende da capacidade de competir com a sofisticação da propaganda jihadista. A luta contra a radicalização *online* exige, portanto, uma abordagem integrada, que combine tecnologia, educação, inclusão social e cooperação internacional.

2.3 O processo da radicalização

A literatura converge no entendimento de que a radicalização é um processo e não um evento isolado. É o percurso que conduz determinados indivíduos à discordância política ou religiosa e à legitimação da violência que envolve mudanças graduais nas crenças e nas emoções, decorridas em contextos sociais específicos (Borum, 2011).

A análise de Francisco Gonçalves (2011), ilustra essa passagem como uma cadeia sequencial que parte de uma revolta moral difusa, passa pela cristalização de uma narrativa

binária (nós versus eles) e culmina na integração de microgrupos que normalizam e justificam o recurso à violência.

Um contributo relevante desta análise reside na centralidade atribuída à identidade, aos lugares e à heterogeneidade das vias de recrutamento. No plano identitário, a radicalização é favorecida por experiências de ambivalência e perda de pertença, que abrem uma janela cognitiva para narrativas radicais, oferecidas por empreendedores ideológicos e redes de ativistas (Gonçalves, 2011).

No plano da causalidade, o autor sublinha que as mesquitas e as prisões não são causas em si de radicalização, mas sim contextos onde, na presença de lacunas institucionais, pequenos grupos podem capturar rotinas, linguagem e autoridade moral, acelerando o processo de radicalização. Por fim, a *Internet* e as redes sociais funcionam, simultaneamente, como lugar de socialização (comunidades de reforço) e como vetor de difusão (propaganda, capacitação técnica, etc.), mitigando o contraditório (Gonçalves, 2011).

A literatura internacional reforça e diversifica este entendimento. O modelo de Moghaddam (2005) concetualiza uma sequência em degraus que liga as condições de isolamento, privação e sentimento de injustiça a uma moralização da violência e à adesão a organizações que a legitimam. Para o autor, não basta desenvolver políticas direcionadas para os indivíduos que se encontram no último degrau (radicalizados), mas sim a adoção de políticas preventivas que abarquem os vários níveis.

Existem outras correntes complementares que descrevem um padrão no processo de radicalização, onde o sentimento de pertença e de identidade se sobrepõe à doutrina: as crises de identidade desencadeiam uma espécie de abertura cognitiva, a qual é explorada por redes de militantes através de processos de seleção, estudo e disciplina, até que a narrativa do grupo se torne o principal filtro de leitura (Hafez & Mullins, 2015).

Em síntese, o processo de radicalização deve ser entendido como uma confluência de mecanismos de diferentes naturezas (social, psicológica) mais do que como uma trajetória linear universal. Com foco na teoria dos movimentos sociais, as crises pessoais ou as tensões identitárias podem gerar uma abertura cognitiva que torna o indivíduo recetivo a novos quadros interpretativos e, nessa altura, as redes organizadas atuam através da mobilização ideológica coletiva para integrá-lo ao movimento (Borum, 2011).

A integração destas leituras permite apresentar um mapa processual combinado em quatro fases. Em primeiro lugar, a fase da abertura cognitiva surge quando ruturas pessoais (fracassos, humilhações, lutos) e injustiças percecionadas tornam desejável uma narrativa ordenadora e moralmente robusta (Hafez & Mullins, 2015).

Em segundo lugar, o enquadramento narrativo e a pertença grupal reorganizam a perceção em binários morais, substituem ambiguidades identitárias por identidades radicais e introduzem novas rotinas e disciplina. (Gonçalves, 2011).

Em terceiro lugar, a normalização e a disciplina são estabilizadas no microgrupo, que fornece a linguagem, os rituais, os limites de informação e as recompensas simbólicas em conformidade, onde a ideologia deixa de ser uma coleção de ideias abstratas e passa a ser uma gramática de vida quotidiana (McCauley & Moskalenko, 2008).

Em quarto lugar, a capacitação e a passagem ao ato resultam da combinação entre a justificação moral amadurecida e acesso a conhecimentos práticos (táticas, recursos e contactos), muitas vezes mediados por ecossistemas digitais (Moghaddam, 2005).

Considera-se, assim, que é nesta etapa que a ação pode ser levada a cabo por atores solitários em linha com a lealdade aos "novos" (aspas do autor) valores e crenças já incorporadas e, portanto, dentro da matriz *jihadista* e em linha com o modelo descentralizado corporizado pelo Daesh ou pela *Al-Qaeda*.

Gonçalves acrescenta um ponto de análise que se revelou particularmente útil no contexto atual: a coexistência entre recrutamento orientado e auto-recrutamento. No primeiro, as redes identificam indivíduos vulneráveis, cultivam os vínculos e definem compromissos; no segundo, são os próprios indivíduos que procuram ativamente conteúdos e grupos, num processo de autoformação independente até convergirem com células ou atuarem de modo autónomo (Gonçalves, 2011).

Esta "dupla via" (aspas do autor) ganha um especial relevo com a ubiquidade das plataformas digitais, nas quais profissionais e amadores produzem e redistribuem conteúdos que combinam apelos emocionais, justificações teológicas, narrativas de vitimização e repertórios tático-operacionais. A desinformação e a ausência de regulação, intensificam a exposição seletiva, reforça a confirmação de crenças e reduz o contacto com contraditório certificado, acelerando as trajetórias de auto-recrutamento (McCauley & Moskalenko, 2008).

Na especificidade da radicalização jihadista, a estrutura do processo não assume um papel central, sendo mais relevante o conteúdo e a intensidade das narrativas. O conteúdo ideológico enfatiza a escatologia e a identidade da comunidade de crentes (*Ummah*), associadas a um enredo de agressão sistémica contra o Islão e a promessas de redenção e heroísmo (Gonçalves, 2011).

As tendências europeias sugerem que a propaganda e a inspiração *online* continuam a desempenhar um papel central, mesmo quando os fluxos organizacionais se tornam

voláteis e quando outras ameaças (p. ex., extremismo de direita e de esquerda) ganham visibilidade (Europol, 2025a). Isso reforça a leitura multidisciplinar do processo e a necessidade de políticas que combinem instrumentos regulatórios, tecnológicos, educativos e comunitários.

Do ponto de vista das políticas de prevenção contra a radicalização terrorista, a literatura tem demonstrado que não existe um único caminho de intervenção, mas sim múltiplas janelas de oportunidade distribuídas ao longo do percurso, correspondendo às dimensões primária, secundária e terciária de prevenção, consoante o estádio do processo (Radicalisation Awareness Network, 2019; Borum, 2011; Hafez & Mullins, 2015). Uma espécie de arquitetura preventiva multinível é coerente com o mapa combinado em quatro fases do processo de radicalização, conforme descrito anteriormente, ou seja, se a radicalização é um processo sequencial, a prevenção tem que ser multidisciplinar e calibrada aos contextos.

O processo de radicalização, tal como descrito neste subcapítulo, assenta historicamente em dinâmicas de proximidade: redes de amizade, mentores carismáticos, socialização em espaços de culto ou em prisões. Nesse sentido, a radicalização foi concebida sobretudo como uma experiência presencial, sustentada por vínculos interpessoais e por rotinas grupais.

A evolução tecnológica e a massificação das plataformas digitais incorporaram uma mutação neste quadro. Muitos dos mecanismos descritos nos modelos tradicionais (abertura cognitiva, enquadramento ideológico, disciplina grupal e capacitação técnica), encontram hoje equivalência direta no espaço *online*. As redes sociais, os fóruns e as aplicações encriptadas passaram a desempenhar o papel das mesquitas virtuais ou das comunidades digitais, onde os indivíduos não consomem apenas propaganda, mas também encontram os seus pares, validam identidades e constroem sentimentos de pertença (Conway, 2017; Radicalisation Awareness Network, 2019).

Na verdade, o plano digital não substitui as dinâmicas *offline*, mas acaba por ampliar o seu alcance, reduzir as barreiras de acesso e acelerar os tempos de socialização. Tal como resulta da análise ao relatório TE-SAT (Europol, 2025a), a propaganda jihadista contemporânea depende cada vez mais de ecossistemas digitais descentralizados, onde a inspiração e o recrutamento por iniciativa própria ocupam o espaço que outrora estava reservado ao contacto direto com as redes organizadas.

3. PERSPETIVAS

3.1 Tendências Evolutivas da Radicalização *online*

A centralidade da *internet* na radicalização jihadista pode ser compreendida à luz da transformação sociológica perante a emergência da sociedade em rede (Castells, 2002). Segundo o autor, o impacto da internet não reside apenas na velocidade da comunicação, mas sobretudo na forma como ela reorganiza a comunidade em torno de afinidades e das escolhas individuais.

Esta perspetiva é particularmente útil para analisar os atuais ecossistemas jihadistas digitais, onde fóruns, redes sociais e aplicações encriptadas funcionam como mesquitas virtuais. O que antes era dependente das interações presenciais em prisões ou círculos de estudo religiosos, é agora amplificado por comunidades virtuais transnacionais, onde a socialização, o reforço identitário e a legitimação da violência ocorrem em rede e em tempo real.

A radicalização jihadista no espaço digital tem sofrido mutações significativas na última década, acompanhando a transformação do ecossistema tecnológico e dos hábitos de consumo mediático. A primeira tendência identificada é a fragmentação e descentralização das plataformas. Se no auge do *Daesh* a difusão propagandística privilegiava as plataformas abertas como *Twitter* ou *Facebook*, atualmente observa-se uma migração consistente para aplicações encriptadas, fóruns privados e até ambientes de *gaming* (Europol, 2025a). Esta realidade reflete uma dupla necessidade: proteger a comunicação do grupo da vigilância das autoridades e manter as comunidades mais homogéneas e controladas, onde a ideologia pode ser reforçada sem contraditório externo.

Uma segunda tendência é a crescente influência dos algoritmos e da inteligência artificial na exposição seletiva dos conteúdos e na formação de "câmaras de eco digitais" (aspas do autor). Diferentemente da propaganda clássica, que dependia da distribuição ativa de materiais impressos ou audiovisuais, o ambiente digital funciona com lógicas de personalização de algoritmos, levando as plataformas a privilegiar conteúdos que maximizam a atenção e o tempo de visualização dos utilizadores (Farber, 2025). Este filtro invisível fomenta uma sobre-exposição a narrativas homogéneas, que reforçam identidades políticas ou religiosas pré-existentes e reduzem o contacto com perspetivas divergentes (Conway, 2017). No campo jihadista, esta dinâmica é particularmente eficaz porque combina três elementos: a disponibilidade constante de materiais extremistas; a interação com pares

que partilham valores semelhantes; e a validação social gerada pelas comunidades digitais sintonizadas que partilham e comentam conteúdos violentos (Awan, 2017).

O relatório TE-SAT (Europol, 2025a) alerta, por exemplo, que a proliferação de inteligência artificial generativa já permite a criação de conteúdos falsificados, os *deepfakes* ou vídeos manipulados e que ampliam a atratividade da propaganda jihadista, dificultando a distinção entre informação legítima e desinformação. Estes produtos digitais não só aumentam a sofisticação visual da propaganda, como também potenciam a sua disseminação viral. Whittaker et al. (2021) acrescentam que este processo deve ser entendido como uma interação contínua entre utilizadores e plataformas, onde cada clique, pesquisa ou partilha retroalimenta o sistema de recomendação, intensificando percursos de radicalização que, em alguns casos, podem culminar na mobilização violenta.

Assim, a influência dos algoritmos e da inteligência artificial não se limita a potenciar a difusão de mensagens extremistas, contribuindo também para a criação de ecossistemas digitais fechados, nos quais o extremismo se normaliza e os utilizadores vulneráveis são, progressivamente, levados a considerar a violência como uma opção legítima.

Uma terceira tendência passa pela inovação nos formatos de propaganda jihadista, com a adoção de ferramentas digitais adaptadas às lógicas de comunicação contemporâneas. Enquanto no passado o foco da comunicação jihadista recaía em revistas digitais extensas como a *Inspire* e a *Dabiq*, hoje verifica-se uma aposta crescente em formatos curtos e visuais altamente sensacionalistas, adaptados às lógicas das redes sociais contemporâneas. Autores como Ingram, et al. (2020) descrevem como o Estado Islâmico sempre procurou adaptar as suas mensagens aos meios digitais dominantes nas sociedades ocidentais, observação que se constata nos relatórios mais recentes das autoridades europeias, onde sublinham a adoção de *memes*, *podcasts*, vídeos curtos ao estilo do *TikTok* e até *deepfakes* para a manipulação digital (Europol, 2025a).

Estes formatos apelam sobretudo às gerações mais jovens, habituadas a um consumo instantâneo e visual de informação, permitindo a normalização do discurso extremista através de códigos visuais contemporâneos.

Verifica-se também a emergência de um modelo de radicalização "*onlife*", conceito que remete para a fusão entre as esferas *online* e *offline* em contextos híbridos de socialização. Neste quadro, a *internet* deixa de ser apenas uma plataforma de difusão de propaganda e passa a constituir-se como um espaço de vida, no qual as relações virtuais e presenciais se entrelaçam e reforçam-se mutuamente (Floridi, 2015).

Tal como foi discutido anteriormente, este fenómeno demonstra que o ambiente digital não substitui os mecanismos tradicionais de radicalização, mas atua em continuidade com eles. Assim, a fase de abertura cognitiva, frequentemente associada a crises identitárias, pode ser acelerada pela via *online* através do contacto com narrativas jihadistas; a procura de pertença é satisfeita por redes de pares virtuais; e a legitimação do uso da violência é consolidada em interações digitais que reforçam as normas grupais. O resultado é um percurso híbrido que encurta os tempos de socialização, reduz as barreiras de entrada para potenciais recrutas e expande as possibilidades do recrutamento por iniciativa própria à escala global (Conway, 2017).

Neste sentido, a radicalização *onlife* constitui um desafio acrescido para a segurança interna, pois implica a vigilância e a monitorização no ciberespaço e, em simultâneo, uma intervenção preventiva nas comunidades locais, onde os sinais do extremismo podem manifestar-se inicialmente de forma encoberta, podendo mais tarde materializar-se em comportamentos de risco no mundo real.

3.2 O plano Europeu e Nacional no Combate à Radicalização *online*

A resposta europeia ao fenómeno da radicalização *online* tem evoluído de forma significativa na última década, refletindo assim o reconhecimento de que as plataformas digitais constituem hoje um dos principais vetores de disseminação da ideologia jihadista e da mobilização violenta. O quadro jurídico da União Europeia foi reforçado com a aprovação do Regulamento n.º 2021/784, do Parlamento Europeu e do Conselho, relativo à remoção de conteúdos terroristas em linha, que entrou em vigor em junho de 2022. Este diploma estabelece que os prestadores de serviços de alojamento devem remover ou bloquear o acesso a conteúdos terroristas no prazo máximo de uma hora após a emissão de uma ordem de remoção por uma autoridade nacional competente, conforme previsto no artigo 3.º do mesmo Regulamento.

Este Regulamento procura equilibrar a proteção da segurança pública com a salvaguarda da liberdade de expressão e informação, impondo também obrigações de transparência e de prestação de contas às plataformas. Este documento vinculativo surge num contexto de crescente fragmentação das redes jihadistas, em que a propaganda e a comunicação operativa migraram para ambientes encriptados e descentralizados, tornando a deteção e a remoção de conteúdos mais complexas.

A Europol (2025a) sublinha que, apesar da implementação do novo enquadramento jurídico, o desafio permanece elevado, devido à rápida replicação e redistribuição dos conteúdos extremistas através de canais alternativos e servidores redundantes.

Complementarmente, a UE tem apostado em estruturas cooperativas destinadas à partilha de informação e à coordenação de respostas. Entre estas destaca-se a *Internet Referral Unit* (EU IRU), integrada no Centro Europeu de Combate ao Terrorismo (ECTC) da Europol, responsável por identificar e reportar conteúdos terroristas às plataformas digitais.

De acordo com o *Internet Referral Unit Transparency Report* 2023 (Europol, 2025b) e no âmbito da aplicação do Regulamento UE 2021/784, em 2023 os Estados Membros transmitiram "329 ordens formais de remoção" (*Removal Orders, ROs*) e "35 164 notificações" (*Referrals*) a prestadores de serviços de alojamento através da *Platform for Exchange on Removal and Countering Illegal Content* (PERCI) (Europol, 2025b, p. 10). Esta plataforma foi desenvolvida pela Europol em parceria com a Comissão Europeia para assegurar a execução rápida e segura das ordens de remoção, permitindo que os conteúdos identificados como terroristas sejam eliminados.

Estes dados ilustram o aumento da capacidade operacional e tecnológica da União Europeia no combate à radicalização e propaganda jihadista *online*. A integração de sistemas automatizados de deteção, conjugada com a coordenação entre os Estados-Membros e as plataformas digitais, reflete uma mudança significativa no paradigma de resposta, ou seja, de uma atuação reativa para uma gestão digital proativa, centrada na remoção célere e na prevenção de *reupload* de conteúdos extremistas (Comissão Europeia, 2024a).

No que diz respeito à prevenção, a UE consolidou um modelo de intervenção através do *EU Knowledge Hub on Prevention of Radicalisation*, lançado pela Comissão Europeia em 2024 como sucessor da *Radicalisation Awareness Network* (Comissão Europeia, 2024b). Este *Hub* funciona como uma plataforma de cooperação entre Estados Membros, investigadores e profissionais especializados, promovendo a partilha de práticas baseadas em evidências para prevenir e mitigar processos de radicalização.

No domínio digital, este modelo assume uma relevância particular, onde o paradigma da prevenção deixa de se limitar à remoção de conteúdos extremistas, passando a integrar o desenvolvimento de contra-narrativas credíveis, a promoção de espaços digitais inclusivos e o reforço das competências digitais dos utilizadores, reconhecendo que a segurança interna depende tanto da resiliência social, como da capacidade tecnológica de resposta.

3.2.1 Espanha no quadro europeu de prevenção da radicalização *online*

Da análise ao relatório TE-SAT (Europol, 2025a), Espanha destaca-se como um dos Estados-Membros com maior número de detenções relacionadas com o terrorismo jihadista, mantendo uma abordagem proativa e preventiva centrada na deteção precoce e no desmantelamento das redes de radicalização digital. O documento reconhece ainda o papel de Espanha no reforço da cooperação europeia em matéria de investigação cibernética e na aplicação do Regulamento (UE) 2021/784, que impõe a remoção célere de conteúdos terroristas *online*.

A política espanhola de combate ao extremismo digital baseia-se numa estratégia integrada que articula intervenção policial, cooperação internacional e prevenção social, integrando na plenitude as políticas e estratégias europeias. Sob a coordenação do *Centro de Inteligencia contra el Terrorismo y el Crimen Organizado* (CITCO), foi criada a *Unidad Nacional de Eliminación de Contenidos Ilícitos* (UNECI), responsável por operacionalizar o Regulamento europeu no território espanhol (CITCO, 2025).

A título de exemplo e de acordo com dados oficiais do Ministério do Interior, publicados em junho de 2025, a UNECI emitiu 134 ordens de retirada de conteúdos terroristas em 2023-2024, ao abrigo do Regulamento (UE) 2021/784, consolidando a posição de Espanha entre os países mais ativos na aplicação do mecanismo europeu de remoção e prevenção de propaganda jihadista, uma vez que, das 134 ordens de retirada de conteúdos terroristas, 85 (cerca de 63%) têm correspondência com conteúdos jihadistas (CITCO, 2025).

Para além das remoções, a Policia Nacional e a Guarda Civil continuam a realizar operações regulares contra indivíduos implicados na produção, consumo e disseminação de conteúdos extremistas *online*, muitas vezes ligados a estruturas de apoio ideológico ao *Daesh* e à *Al-Qaeda*.

Esta estratégia de intervenção e de remoção de conteúdos está alinhada com o paradigma de resiliência e resposta integrada da UE. Esta abordagem exemplificativa reflete a incidência dos conteúdos jihadistas na esfera digital no continente europeu e, em particular, em Espanha.

3.2.2 O contexto em Portugal: Estruturas e Desafios

No quadro do Regulamento (UE) 2021/784, relativo à luta contra a difusão de conteúdos terroristas em linha, Portugal ainda não identificou as suas autoridades nacionais

competentes e os pontos de contacto à Comissão Europeia, para que possa integrar a lista de países com capacidade para atuar nos termos do Regulamento (Comissão Europeia, 2025a).

Considera-se que este atraso pode fragilizar a capacidade de resposta imediata a casos de disseminação de propaganda jihadista ou conteúdos extremistas em plataformas digitais, dificultando também a integração plena de Portugal nos mecanismos de cooperação e partilha de informação liderados pela Europol.

Este cenário encontra paralelo noutras áreas da cibersegurança. A título de exemplo, a Diretiva (UE) 2022/2555, conhecida como NIS 2, que estabelece medidas destinadas a alcançar um elevado nível comum de segurança das redes e da informação em toda a União, deveria ter sido transposta para o ordenamento jurídico nacional até 17 de outubro de 2024, contudo ainda não foi publicado o diploma correspondente (Comissão Europeia, 2025b).

A ausência de transposição atempada demonstra uma tendência de atraso regulatório e da baixa priorização política no domínio da segurança digital, que pode comprometer a coerência entre as políticas europeias de prevenção da radicalização *online* e as de resiliência cibernética.

Apesar de Portugal ainda não ter comunicado as autoridades competentes nos termos do Regulamento 2021/784, constata-se pela publicação no diário da Assembleia da República, de 03 de outubro de 2025, que a Polícia Judiciária (PJ) será a entidade responsável para efeitos de emissão de decisões de supressão ou de bloqueio de conteúdos em linha, nos termos do artigo 3.º do Regulamento (Decreto da Assembleia da República N.º 10/XVII, 2025). Embora a legislação nacional esteja em adaptação ao Regulamento (UE) 2021/784, não existem relatórios oficiais com dados sobre a execução de ordens de remoção.

A Estratégia Nacional de Combate ao Terrorismo (ENCT 2023), aprovada pela Resolução do Conselho de Ministros n.º 40/2023, redefine a política nacional nesta matéria à luz da evolução tecnológica e geopolítica. Estruturada em quatro eixos estratégicos (prevenção, proteção, perseguição e resposta), a ENCT 2023 introduz duas prioridades transversais particularmente relevantes para o tema da radicalização *online*: o reforço da vigilância e da defesa no ciberespaço e a deteção precoce de fatores de vulnerabilidade individual, incluindo problemas de saúde mental suscetíveis de potenciar processos de radicalização (Presidência do Conselho de Ministros, 2023).

A coordenação das medidas antiterroristas é assegurada pela Unidade de Coordenação Antiterrorista (UCAT), criada no âmbito do Sistema de Segurança Interna (SSI), conforme plasmado na Lei de Segurança Interna, sendo constituída por representantes das forças e serviços de segurança: Guarda Nacional Republicana (GNR), Polícia de

Segurança Pública (PSP), Polícia Judiciária (PJ), Sistema de Informações Estratégicas de Defesa (SIED), Sistema de Informações de Segurança (SIS) e Polícia Marítima (PM).

Embora a UCAT não possua competências diretas sobre conteúdos digitais, funciona como um centro de fusão de inteligência e desempenha um papel crucial na partilha de informações na área do terrorismo. Para além disso, é a unidade responsável pela implementação dos planos de ação previstos na ENCT 2023, destacando-se o Plano de Ação de Prevenção da Radicalização e dos Extremismos Violentos e do Recrutamento para o Terrorismo.

Este plano tem como principal objetivo prevenir e antecipar a mobilização de indivíduos para a prática de atos suscetíveis de configurarem infrações terroristas ou extremistas violentas e atividades conexas com estes fenómenos. O plano encontra-se em fase de revisão, sem versão pública disponível.

No que diz respeito às principais entidades nacionais com responsabilidade na área do terrorismo e na radicalização, destaca-se o Serviço de Informações de Segurança (SIS) que mantém responsabilidade primária na identificação e avaliação de ameaças internas relacionadas com o terrorismo, de acordo com a Lei n.º 9/2007, de 19 de fevereiro, que aprova o regime jurídico do Sistema de Informações da República Portuguesa (SIRP). Compete-lhe, entre outras funções, produzir informações que contribuam para a salvaguarda da segurança interna e prevenir atos de sabotagem, espionagem e terrorismo (artigo 4.º).

Também sobre a dependência do SIRP, o SIED tem como missão principal a produção de informações relevantes para a salvaguarda da independência nacional, dos interesses estratégicos do Estado e da segurança externa, conforme disposto na Lei n.º 9/2007, de 19 de fevereiro, e regulamentado pelo Decreto-Lei n.º 4/2014, de 13 de janeiro. Ao contrário do SIS, que atua predominantemente no plano interno, o SIED centra-se na monitorização de ameaças externas, incluindo redes terroristas transnacionais, fluxos ilícitos e dinâmicas geopolíticas que possam afetar a segurança nacional. A sua função de recolha e análise estratégica de informação de origem externa é fundamental para antecipar riscos e apoiar a coordenação com parceiros internacionais. No domínio da radicalização jihadista, o SIED contribui para a avaliação das conexões transfronteiriças e digitais de grupos extremistas, fornecendo uma perspetiva estratégica que complementa a atuação operacional do SIS e de todas as entidades que integram a UCAT.

A PJ, por sua vez, detém competência exclusiva para a investigação criminal das infrações terroristas, conforme estabelecido na Lei de Organização da Investigação Criminal

(Lei n.º 49/2008, de 27 de agosto), em estreita articulação com a Europol e as autoridades judiciárias nacionais.

As forças de segurança, designadamente a PSP, GNR e a PM, desempenham igualmente um papel relevante no campo da prevenção, dissuasão e resposta, através da vigilância de locais sensíveis, da proximidade comunitária e da recolha de informações sobre eventuais sinais de radicalização. Através das suas unidades de informações e de investigação criminal, estas forças, em comunhão com as demais entidades que integram a UCAT, são fundamentais na deteção e resposta a comportamentos suspeitos e na proteção de alvos estratégicos e das infraestruturas críticas, contribuindo assim para uma abordagem integrada da segurança interna e prevenção do terrorismo.

Na esfera digital, para além das entidades que integram a UCAT, importa ainda destacar o Gabinete Nacional de Segurança (GNS), criado pelo Decreto-Lei n.º 3/2012, de 16 de janeiro, que exerce funções no domínio da proteção da informação classificada e da segurança das redes e sistemas de comunicação do Estado, sendo também a autoridade nacional para a aplicação das normas da NATO e da União Europeia em matéria de segurança da informação.

No âmbito do GNS funciona o Centro Nacional de Cibersegurança (CNCS), responsável pela coordenação operacional da cibersegurança nacional e atua como autoridade nacional competente para efeitos da Diretiva NIS.

Estas entidades compõem um ecossistema institucional diversificado que, embora concebido para garantir uma abordagem abrangente à segurança interna, enfrenta o desafio da dispersão de competências e da necessidade de uma coordenação efetiva, especialmente no domínio da radicalização *online*.

O artigo 4.º da Lei de Combate ao Terrorismo (Lei n.º 52/2003, alterada pela Lei n.º 2/2023) demonstra um avanço normativo na incriminação do treino técnico e da aquisição de meios para a prática de atos terroristas por iniciativa própria, mas persiste uma omissão estrutural quanto à dimensão ideológica da radicalização e inspiração pela via digital.

A norma centra-se no treino material, ou seja, fabrico de armas, explosivos ou técnicas de ataque, ignorando as formas contemporâneas de treino ideológico e de inspiração à radicalização, amplamente difundidas nas plataformas digitais jihadistas.

Em sentido oposto, o quadro jurídico europeu através do Regulamento (UE) 2021/784, reconhece e pune também o incitamento indireto e a apologia de atos terroristas, incorporando dimensões simbólicas e cognitivas da radicalização.

Esta discrepância limita a capacidade de intervenção precoce das autoridades nacionais e enfraquece a coerência entre a lei penal e as estratégias de prevenção.

Recomenda-se para a futura alteração da Lei de Combate ao Terrorismo a inclusão do treino ideológico, a intenção direta e indireta, em articulação com os instrumentos europeus reforçando a eficácia da resposta nacional perante as novas dinâmicas da radicalização *online*.

Em síntese, o panorama português revela avanços normativos e institucionais relevantes, mas também lacunas estruturais que podem limitar a resposta à radicalização *online*. O desafio futuro reside em transformar estas fragilidades em oportunidades de cooperação e inovação no domínio da segurança interna digital.

4. CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu demonstrar que a radicalização jihadista, particularmente no ambiente digital, constitui um fenómeno híbrido e evolutivo, que combina dimensões ideológicas, tecnológicas e sociais. A evolução do terrorismo jihadista reflete uma sofisticação crescente em diferentes planos (estratégico, comunicacional e simbólico), que exige respostas igualmente complexas e multidimensionais.

A propaganda digital jihadista, em particular, continua a representar uma ameaça dinâmica e adaptável, com grande capacidade de inovação e disseminação de conteúdos extremistas. A compreensão profunda das suas estratégias comunicacionais, especialmente na relação entre o território e a narrativa digital, é indispensável para conceber respostas políticas e operacionais ajustadas. A sofisticação técnica do jihadismo contemporâneo obriga, portanto, a uma vigilância constante sobre as mutações do ecossistema digital, onde a propaganda e o recrutamento coexistem com processos de socialização.

No plano teórico, a integração entre o modelo de Gonçalves (2011) e a literatura internacional sustenta uma definição robusta de radicalização como trajetória social e cognitiva, marcada por fases e mecanismos que podem, mas não têm que culminar em violência. Assim, a prevenção eficaz requer a identificação precoce dos mecanismos dominantes e a intervenção em várias frentes (educativa, social, clínica e penal), com uma monitorização contínua de resultados (Hafez & Mullins, 2015; Moghaddam, 2005).

No plano europeu, o Regulamento (UE) 2021/784 e a atuação da EU IRU representam passos decisivos na institucionalização de um modelo cooperativo de combate à difusão de conteúdos terroristas *online*. A criação do *EU Knowledge Hub on Prevention of*

Radicalisation reforça esta abordagem, integrando dimensões jurídicas, tecnológicas e sociais num quadro de prevenção multinível (Comissão Europeia, 2024b). Apesar destes avanços, subsistem desafios estruturais: a natureza mutável das plataformas digitais, a descentralização dos ecossistemas jihadistas e a necessidade de equilibrar a segurança pública com a salvaguarda dos direitos fundamentais.

O exemplo da realidade espanhola ilustra bem as assimetrias na aplicação das políticas europeias. Espanha destaca-se pelo modelo integrado de resposta, que conjuga investigação, prevenção e cooperação internacional, através da ação da UNECI e da coordenação do CITCO (2025). Já Portugal, embora disponha de uma estrutura institucional e de um enquadramento estratégico suportado na ENCT 2023, verifica-se uma segregação de entidades competentes e atrasos na designação das autoridades competentes para o Regulamento (UE) 2021/784, bem como na transposição da Diretiva NIS 2 (Comissão Europeia, 2025a; 2025b).

A coordenação entre a UCAT e o CNCS assume particular relevância, na medida em que pode favorecer a complementaridade entre capacidades tecnológicas, operacionais e preventivas, reforçando a coerência da resposta nacional ao extremismo digital.

Importa nesta fase, reconhecer os condicionalismos e limitações deste estudo, decorrentes da natureza sensível e reservada do fenómeno em análise. O acesso restrito a informação classificada e a dados operacionais das autoridades nacionais e europeias condicionou a possibilidade de uma análise mais aprofundada. Acrescem as limitações inerentes ao formato académico, que impuseram uma seleção criteriosa das fontes.

Em síntese, o enquadramento europeu e nacional para o combate à radicalização *online* demonstra um avanço normativo considerável, mas enfrenta desafios persistentes. A eficácia futura dependerá da capacidade dos Estados-Membros em garantir coerência entre os níveis europeu, nacional e local, e em promover uma cultura de prevenção digital que envolva a sociedade no seu todo. Mais do que uma questão de segurança pública, a radicalização jihadista *online* é um desafio social, que interpela o Estado, as instituições e os cidadãos.

Na esperança de que os assuntos abordados poderão contribuir para o desenvolvimento de estudos mais aprofundados, abre-se a reflexão sobre a possibilidade de atribuição de competências em matéria de cibersegurança ao SSI, atendendo à abordagem integrada, multidisciplinar, colaborativa e capaz de conjugar a prevenção, investigação e a resposta a incidentes, que esta camada da segurança interna (digital) requer.

Em última análise, a resposta a este fenómeno exige assim, o reforço da resiliência democrática e da coesão social para contrariar a violência ideológica e proteger a segurança interna num mundo cada vez mais digitalizado, considerando-se fundamental a construção de um modelo integrado de segurança interna que combine inovação tecnológica, coordenação interinstitucional e prevenção. Como lembra Germano Marques da Silva, "por muito boas que sejam as leis, para além das leis importa o modo como são aplicadas, o espírito que anima todos os que participam neste combate." (Silva, 2019, p. 289).

BIBLIOGRAFIA

Arena, M. d. (2022). Duas Versões da Jihad? Análise do Pensamento, Objetivos e Estratégias do Daesh e da Al-Qaeda. Em Instituto da Defesa Nacional, Nação e Defesa, *Conflitos Armados* (161 ed., pp. 9-32). Obtido de https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD161/NeDef161_1_MariaCeuPintoArena.pdf

Awan, I. (2017). Cyber-extremism: ISIS and the power of social media. *Social Science and Public Policy, 54*, pp. 138-145. doi:10.1007/s12115-017-0114-0

Bartlett, J., & Miller, C. (2011). The Edge of Violence: Towards Telling the Difference Between Violent and Non-Violent Radicalization. *Terrorism and Political Violence, Vol. 24*, pp. 1-21. doi:10.1080/09546553.2011.594923

Borum, R. (2011). Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security, 4*, pp. 7-36. doi:10.5038/1944-0472.4.4.1

Castells, M. (2002). *The Internet Galaxy. Reflections on the Internet, Business, and Society.* Oxford: Oxford University Press.

CITCO. (2025). *Informe de Transparencia 2023-2024, Retirada de contenidos terroristas*. Ministério do Interior. Obtido de https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2024/Informe_Retirada_Contenidos_Terroristas_CITCO.pdf

Cockburn, P. (2014). *Jihadis Return: ISIS and the New Sunni Uprising.* OR Books.

Comissão Europeia. (2024a). Relatório da Comissão ao Parlamento Europeu e ao Conselho sobre a implementação do Regulamento (UE) 2021/784 relativo à luta contra a difusão de conteúdos terroristas em linha [COM(2024) 64 final]. Publications Office of the European Union. Obtido de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0064

Comissão Europeia. (2024b). Comunicado de 18-06-2024. *Commission launches the new EU Knowledge Hub on Prevention of Radicalisation*. Obtido de https://home-affairs.ec.europa.eu/news/commission-launches-new-eu-knowledge-hub-prevention-radicalisation-2024-06-18_en

Comissão Europeia. (2025a). Comunicação de 25 de setembro de 2025. *List of national competent authority (authorities) and contact points*. Obtido de https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-

radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en?prefLang=pt

Comissão Europeia. (2025b). Comunicado a 7 de maio de 2025. *Commission calls on 19 Member states to fully transpose the NIS2 Directive*. Obtido de https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive

Conway, M. (2017). Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflit & Terrorism, Vol. 40*, pp. 77-98. doi:10.1080/1057610X.2016.1157408

Davis, B. R. (2006). Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance. *CommLaw Conspectus - Journal of Communications Law and Policy, 15*(1), 119-185. Obtido de https://scholarship.law.edu/commlaw/vol15/iss1/7/

Decreto da Assembleia da República N.º 10/XVII. (2025). Diário da Assembleia da República, II Série-A, Número 75, de 03 de outubro de 2025. *Autoriza o Governo a adaptar a Ordem Jurídica Interna ao 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*. Obtido de https://debates.parlamento.pt/catalogo/r3/dar/s2a/17/01/075S1/2025-10-03/5?pgs=5-6&org=PLC&plcdf=true

Decreto-Lei n.º 248/95, de 21 de setembro - Cria na estrutura do Sistema da Autoridade Marítima, a Polícia Marítima. (s.d.). Obtido de Diário da República n.º 219/1995, Série I-A de 1995-09-21, páginas 5890 - 5896: https://diariodarepublica.pt/dr/detalhe/decreto-lei/248-1995-566656

Decreto-Lei n.º 3/2012, de 16 de janeiro - Aprova a orgânica do Gabinete Nacional de Segurança. (s.d.). Obtido de Diário da República n.º 11/2012, Série I de 2012-01-16, páginas 174 - 177: https://diariodarepublica.pt/dr/detalhe/decreto-lei/3-2012-544575

Decreto-Lei n.º 69/2014, de 9 de maio - Estabelece os termos e o funcionamento do CNCS. (s.d.). Obtido de Diário da República n.º 89/2014, Série I de 2014-05-09, páginas 2712 - 2719: https://diariodarepublica.pt/dr/detalhe/decreto-lei/69-2014-25343754

Duarte, F. P. (2015). *Jihadismo Global - Das Palavras aos Atos.* Marcador.

Europol. (2025a). *European Union Terrorism Situation and Trend Report (EU TE-SAT).* Publications Office of the European Union. Obtido de

https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2025-eu-te-sat

Europol. (2025b). *2023 EU IRU Transparency Report.* Luxembourg: Publications Office of the European Union. Obtido de https://www.europol.europa.eu/publications-events/publications/eu-internet-referral-unit-transparency-report-2023

Farber, S. (2025). AI-Enabled Terrorism: A Strategic Analysis of Emerging Threats and Countermeasures in Global Security. *Journal of Strategic Security*, pp. 320-344. Obtido de https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2377&context=jss

Fernandes, R. N. (2025). *Outlets de Desinformação na Nova Geopolítica Digital.* Lisboa: ICPOL-ISCPSI.

Fiães Fernandes, L. (2014). *Intelligence e Segurança Interna.* Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

Floridi, L. (2015). *The Onlife Manifesto: Being Human in a Hyperconnected Era.* Springer. doi:10.1007/978-3-319-04093-6

Gonçalves, F. (2011). *O Islamismo Radical e o Combate às suas Ameaças: da Dawa à Jihad.* Loures: Diário de Bordo.

Gray, J. (2003). *Al Qaeda and what it Means to be Modern.* United Kingdom: New Press.

Hafez, M., & Mullins, C. (2015). The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism. *Studies in Conflict & Terrorism, 38*, pp. 958-975. doi:10.1080/1057610X.2015.1051375

Ingram, H. J., Whiteside, C., & Winter, C. (2020). *The ISIS reader: Milestone texts of the Islamic State movement.* Oxford University Press.

Kaczkowski, W., Winkler, C., Damanhoury, K. E., & Luu, Y. (2021). Intersctions of the Real and the Virtual Caliphates: The Islamic State's Territory and Media Campaign. *Journal of Global Security Studies, 6, Issue 2*. Obtido de https://doi.org/10.1093/jogss/ogaa020

L. Bokhari, T. H. (2006). Paths to Global Jihad: Radicalisation and Recruitment to Terror Networks. *FFI Seminar hosted by the Norwegian Defense Research Establishment.* Oslo.

Lei n.º 49/2008, de 27 de agosto - Lei de Organização da Investigação Criminal. (s.d.). Obtido de Diário da República n.º 165/2008, Série I de 2008-08-27, páginas 6038 - 6042: https://diariodarepublica.pt/dr/detalhe/lei/49-2008-453255

Lei n.º 52/2003, de 22 de agosto - Lei de Comabate ao Terrorismo. (s.d.). Obtido de Diário da República n.º 193/2003, Série I-A de 2003-08-22: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2003-34568575

Lei n.º 53/2007, de 31 de agosto - Lei orgânica da Polícia de Segurança Pública. (s.d.). Obtido de Diário da República n.º 168/2007, Série I de 2007-08-31: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2007-174279072

Lei n.º 53/2008, de 29 de agosto - Lei de Segurança Interna. (s.d.). Obtido de Diário da República n.º 167/2008, Série I de 2008-08-29: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2008-34501675

Lei n.º 63/2007, de 6 de novembro - Lei orgânica da Guarda Nacional Republicana. (s.d.). Obtido de Diário da República n.º 213/2007, Série I de 2007-11-06: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2007-107794647

Lei n.º 9/2007, de 19 de fevereiro - Estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança. (s.d.). Obtido de Diário da República n.º 35/2007, Série I de 2007-02-19, páginas 1238 - 1252: https://diariodarepublica.pt/dr/detalhe/lei/9-2007-517985

Matos, H. J. (2016). *Sistemas de Segurança Interna: Terrorismo & Contraterrorismo.* Casal de Cambra: Caleidoscópio.

McCauley, C., & Moskalenko, S. (2008). Mechanisms of Political Radicalization: Pathways Toward Terrorism. *Terrorism and Political Violence, 20*, pp. 415-433. doi:10.1080/09546550802073367

Moghaddam, F. M. (2005). The Staircase to Terrorism: A Psychological Exploration. *American Psychologist, 60*, pp. 161-169. doi:10.1037/0003-066X.60.2.161

Neumann, P. R. (2016). *Radicalized: New jihadists and the threat to the West.* I.B. Tauris & Co Ltd.

OSCE. (2024). *Strengthening media and information literacy in the context of preventing violent extremism and radicalization that lead to terrorism: A focus on South-Eastern Europe.* Organization for Security and Co-operation in Europe (OSCE). Obtido de https://www.osce.org/files/f/documents/4/4/575970.pdf

Pires, N. L. (2016). Do Terrorismo Transnacional ao Choque de Valores. *IDN Nação e Defesa*, pp. 59-70. Obtido de https://revistas.rcaap.pt/nacao/article/view/37768/26098

Presidência do Conselho de Ministros. (2023). Estratégia Nacional de Combate ao Terrorismo. *Aprovada na Resolução do Conselho de Ministros n.º 40/2023, de 3 de maio de 2023*. Obtido de Diário da República n.º 85/2023, Série I de 2023-05-03: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/40-2023-212551390

Quivy, R., & Campenhoudt, L. V. (2005). *Manual de Investigação em Ciências Sociais.* Lisboa: Gradiva.

Radicalisation Awareness Network. (2019). *Preventing radicalisation to terrorism and violent extremism: Approaches and practices.* Publications Office of the European Union. Obtido de https://home-affairs.ec.europa.eu/system/files/2021-05/ran_collection-approaches_and_practices_en.pdf?utm

Rato, V. (03 de outubro de 2016). Nos Desertos de al-Zarqawi, da Al-Qaeda ao "Estado Islâmico". Em Instituto de Defesa Nacional, Defesa e Nação, *Terrorismo Transnacional* (143 ed., pp. 10-42). Obtido de https://revistas.rcaap.pt/nacao/article/view/37696

Shaw, A. (2023). Social media, extremism, and radicalization. . *Science advances, 9 (35), eadk2031., 9 (35), eadk2031.* doi:10.1126/sciadv.adk2031

Shultz, R. H. (2008). Global Insurgency Strategy and the Salafi Jihad Movement. *Institute for National Security Studies*(Occasional Paper N,º 66). Obtido de https://books.google.pt/books?id=0s0gAQAAIAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f

Silva, G. M. (2019). Métodos expeditos de obtenção de prova: os valores democráticos em risco? Em (Coord.): Manuel Valente, *Criminalidade Organizada Transnacional - Corpus Delicti I.* Coimbra: Almedina.

Soares, M. (2013-2014-2015). A radicalização salafista-jihadista na Europa: o caso dos imigrantes de segunda e terceira geração conectados com o Islão. *Politeia, Revista do Instituto Superior de Ciências Policiais e Segurança Interna*, pp. 185-210. Obtido de https://politeia-online.pt/wp-content/uploads/2022/03/A-radicalizacao-salafista-jihadista-na-Europa-_-caso-dos-imigrantes-de-segunda-e-terceira-geracao-conectados-com-o-Islao-pag.185-210.pdf

U.S. S. Committee, Homeland Security, Gov. Affairs. (7 de May de 2015). *Jihad 2.0: Social media in the next evolution of terrorist recruitment*. (U. G. Office, Editor) Obtido de https://archive.org/details/gov.gpo.fdsys.CHRG-114shrg95653/mode/2up

União Europeia. (2021). Regulamento (UE) 2021/784 do Parlamento Europeu e do Conselho, de 29 de abril de 2021, relativo à luta contra a difusão de conteúdos terroristas em linha. *Jornal Oficial da União Europeia, L 172/17.05.21*, 79-109. Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32021R0784

Ventura, J. P., & Carvalho, C. M. (2020). *Da Radicalização Ideológica ao Terrorismo.* Lisboa: Diário de Bordo.

Weimann, G. (2014). *New Terrorism and New Media.* Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars. Obtido de https://www.wilsoncenter.org/publication/new-terrorism-and-new-media

Whittaker, J., Looney, S., Reed, A., & Votta, F. (2021). Recommender systems and the amplification of extremist content. *Internet Policy Review, 10*. doi:10.14763/2021.2.1565