Revista Latino-Americana de RELAÇÕES INTERNACIONAIS Campos Neutrais
FURG UNIVERSIDADE FEDERAL DO RIO GRANDE
ARTIGO

Terrorismo na Era Digital: Desafios Jurídicos e Éticos para a Segurança Internacional e o Estado de Direito

The Challenge of Terrorism in the Modern Era: Legal and Ethical Challenges for International Security and the Rule of Law

Douglas Aparecido Bueno

Resumo

O presente artigo analisa a mutação do terrorismo contemporâneo para um fenômeno atomizado e digitalmente imerso, impulsionado pela hiperconectividade. Discute como essa transformação desafia as normas, instituições e estratégias tradicionais de segurança internacional, erigidas em paradigmas analógicos e estatais. O problema central reside em como as estruturas de segurança podem se adaptar e responder eticamente e eficazmente à difusão do terrorismo digital, sem comprometer os fundamentos do Estado de Direito e as liberdades individuais. A investigação explora a atomização e difusão do terrorismo na era digital, detalhando a radicalização online, o uso da criptografia e o ciberterrorismo, com destaque para a realidade brasileira. Em seguida, avaliamos as limitações das normas e instituições tradicionais de segurança internacional, como a ineficácia da dissuasão contra fatores não estatais e o normativo do direito internacional diante das tecnologias emergentes, abordando o equilíbrio entre segurança e liberdade. Por fim, propõe uma releitura estratégica para uma adaptação ética e eficaz, enfatizando a necessidade de conciliar a segurança com os direitos fundamentais. A metodologia utilizada consiste numa revisão bibliográfica sistemática, com referencial teórico multidisciplinar que integra Direito, Filosofia Política e Relações Internacionais. O estudo conclui que o combate ao terrorismo digital exige um modelo holístico, capaz de inovação tecnológica articular, formação ética e cooperação internacional séria, reafirmando o compromisso com os valores democráticos para evitar que uma resposta estatal se assemelhe à lógica da exceção.

Palavras-chave: terrorismo digital; segurança internacional; criptografia; direitos fundamentais; ciberterrorismo.

Abstract

This paper delves into the evolution of modern terrorism as a decentralized and technology-driven phenomenon, propelled by extensive connectivity. It delves into the implications of this transformation on established conventions, organizations, and approaches to global security, which were crafted within outdated frameworks centered around analog methods and nation-states. The core concern revolves around the ethical and practical adjustments that security frameworks must make to effectively counter the proliferation of digital terrorism while upholding the principles of the Rule of Law and personal liberties. The research explores the fragmentation and dissemination of terrorism in the digital epoch, outlining phenomena like online radicalization, encryption employment, and cyber threats, with a specific focus on the context in Brazil. It then evaluates the constraints of traditional global security standards and bodies, highlighting the inadequacy of deterrence strategies against non-state entities and the regulatory gaps in international law vis-à-vis emerging technologies, addressing the delicate balance between security imperatives and individual freedoms. In conclusion, the paper suggests a strategic reevaluation for a morally sound and efficient adaptation, stressing the importance of harmonizing security imperatives with core rights. The approach adopted involves a comprehensive review of literature grounded in an interdisciplinary framework that merges Law, Political Philosophy, and International Affairs. The study underscores that countering digital terrorism necessitates an integrated approach that bridges technological advancements, ethical considerations, and robust international collaboration, reasserting the commitment to democratic principles to prevent state reactions from veering into exceptional measures.

Keywords: digital terrorism; global security; encrypted communication; core rights protection; cyber threats.

1 INTRODUÇÃO

O terrorismo contemporâneo apresenta uma mutação profunda em sua estrutura e *modus operandi*, configurando-se como um fenômeno atomizado, descentralizado e profundamente imerso no ecossistema digital. A hiperconectividade, resultante da expansão das tecnologias de informação e comunicação, alterou radicalmente a dinâmica da violência política, permitindo que indivíduos e pequenos grupos atuem de forma autônoma, porém articulada, por meio de redes virtuais transnacionais. Diferentemente dos agrupamentos hierárquicos do passado, o terrorismo atual é fluido, deslocalizado e altamente adaptável, representando um desafio inédito para as instituições jurídicas e os sistemas de segurança internacionais erigidos com base em paradigmas analógicos e estatais.

Essa transformação estrutural do terrorismo impõe não apenas um reposicionamento estratégico por parte dos agentes da segurança internacional, mas exige sobretudo uma reconfiguração ética e jurídica no enfrentamento da ameaça. O uso da criptografia, a radicalização online e o advento do ciberterrorismo revelam uma tensão latente entre o imperativo da vigilância e a salvaguarda das liberdades fundamentais. A possibilidade de interceptação, controle e segurança de atos terroristas encontra-se condicionada a dispositivos tecnológicos que, ao mesmo tempo em que protegem a privacidade dos cidadãos, podem ser instrumentalizados para ações especificamente ilícitas e violentas. Tal dilema exige uma resposta que transcenda as soluções técnicas ou repressivas, exigindo reflexão crítica sobre os próprios fundamentos do Estado de Direito em tempos de insegurança difusa.

Nesse contexto, o problema que orienta esta investigação consiste em compreender de que modo as normas, instituições e estratégias tradicionais de segurança internacional podem ser reformuladas e adaptadas para responder, de maneira eficaz e eticamente legítima, às características do terrorismo digitalizado, sem abdicar dos princípios democráticos nem comprometer os direitos individuais. A questão torna-se ainda mais relevante diante da sofisticação dos métodos de radicalização e recrutamento online, do uso intensivo de criptografia para comunicação sigilosa entre atores violentos, e da emergência de ações cibernéticas com potencial destrutivo confirmado ao terrorismo físico tradicional.

A relevância desse debate não se restringe ao âmbito acadêmico, mas reverbera diretamente na formulação de políticas públicas e na cooperação internacional. A segurança,

em um mundo cada vez mais interconectado, não pode ser pensada apenas em termos de proteção territorial, mas deve incorporar as dimensões cibernética, informacional e normativa. Com isso, o enfrentamento do terrorismo exige uma abordagem integrada, multidisciplinar e centrada na dignidade da pessoa humana, recusando soluções que, em nome da segurança, comprometam os valores fundantes da convivência democrática.

Dessa forma, o objetivo central deste artigo é analisar criticamente as possibilidades de proteção normativa e institucional da segurança internacional diante do terrorismo na era digital. Para alcançar tal objetivo, o estudo se apoiará em uma revisão bibliográfica sistemática, de natureza qualitativa, orientada por um referencial teórico multidisciplinar, que articula fundamentos do direito, da filosofia política e das relações internacionais. Ao final, pretendemos oferecer contribuições que conciliem a necessidade de contenção da violência terrorista com a preservação de uma ordem jurídica baseada na liberdade, nos direitos humanos e na responsabilidade ética dos Estados.

2 ATOMIZAÇÃO E DIFUSÃO DO TERRORISMO NA ERA DIGITAL

A ascensão da era digital e a afirmação da hiperconectividade remodelaram profundamente as tendências do terrorismo, conferindo-lhe características inovadoras de dispersão e adaptabilidade. Diferentemente das organizações centralizadas e hierarquicamente organizadas do século XX, o terrorismo contemporâneo tende à atomização: uma multiplicação de atores individuais, muitas vezes desconectados fisicamente, mas integrados por redes digitais globais. Essa descentralização proporciona uma resiliência operacional que desafia os mecanismos tradicionais de vigilância, controle e repressão (Sageman, 2008).

Marc Sageman (2008), em sua obra "Leaderless Jihad"[1], descreve essa nova configuração como uma "jihad sem líderes", operando em redes horizontais com baixa previsibilidade e alta capacidade de regeneração. Os chamados "lobos solitários" ou "células adormecidas" são exemplos dessa fragmentação tática, cujas ações são frequentemente inspiradas por discursos extremistas circulantes no ciberespaço. A fluidez dessas redes dificulta

[1] Embora seminal, a tese de Sageman sobre a "jihad sem líderes" tem sido objeto de debate na academia, com alguns críticos argumentando que ela pode subestimar a persistência de elementos de liderança e organização, ainda que descentralizados, dentro das redes terroristas. Para uma análise crítica, ver: (Roy, 2008)

a identificação de estruturas, financiadores ou articuladores centrais, desafiando os arcabouços jurídicos que ainda se baseiam, em muitos casos, na lógica da perseguição penal tradicional.

No Brasil, essa realidade também se faz presente. Segundo Nascimento e Amaral (2022), o ambiente digital tem ampliado significativamente a capacidade de difusão de ideologias extremistas no país, potencializando a atuação de grupos com agenda violenta. Plataformas como Telegram e redes sociais descentralizadas, como o Gab e o Parler, são usadas por grupos extremistas para disseminar discursos de ódio e coordenar ações. Trata-se de uma simbiose entre a arquitetura das mídias digitais e as estratégias de mobilização terrorista, cujos efeitos escapam às fronteiras nacionais e desafiam a soberania estatal.

A radicalização online se apresenta como um dos fenômenos mais inquietantes da era digital. A facilidade de acesso à informação e a interconexão global, que impulsionaram avanços significativos, também abriram portas para a disseminação de ideologias extremistas e para o engajamento de indivíduos em movimentos radicais.

Estudos de Neumann[2] (2013) revelam que a maior parte dos processos de radicalização contemporâneos ocorre por meio de interações digitais, sem necessidade de contato físico direto. O "ecossistema do ódio" digital alimenta-se da lógica algorítmica das redes sociais, nas quais o engajamento é privilegiado, mesmo quando se trata da propagação de conteúdos extremistas. A velocidade e a escala dessas interações tornam os modelos tradicionais de dissuasão e contenção absolutamente insuficientes.

Outro elemento-chave nesse processo é o uso da criptografia. Ferramentas de comunicação criptografadas, como Signal, Telegram e WhatsApp, garantem a confidencialidade das comunicações privadas, mas também fornecem recursos essenciais para a atuação de grupos terroristas. De acordo com Bocchino (2025), essa infraestrutura digital criptografada permite o planejamento e a execução de atentados com altíssimo grau de invisibilidade, frustrando tentativas de interceptação e monitoramento pelas agências de inteligência. O dilema ético e jurídico aqui se impõe: como proteger a privacidade dos cidadãos sem oferecer garantia à impunidade de ações terroristas? Note-se que além da radicalização e da comunicação protegida, o ciberterrorismo propriamente dito representa uma ameaça cada

[2] A radicalização online é um campo de estudo complexo, com diversas teorias que buscam explicar como indivíduos são influenciados por conteúdos extremistas na internet. Pesquisas contemporâneas apontam para um cenário multifacetado, onde fatores pessoais e dinâmicas de grupo online interagem. Para uma visão abrangente das teorias e desafios conceituais, ver: (Macdonald; Whittaker, 2019).

vez mais concreta. Segundo Dunn Cavelty (2013), o ciberterrorismo é a utilização maliciosa de tecnologias de informação para provocar danos físicos, psicológicos ou estruturais a uma sociedade. Infraestruturas críticas, como redes elétricas, sistemas de abastecimento de água podem e bancos de dados governamentais, serão alvos preferenciais. Em 2020, por exemplo, o Tribunal Superior Eleitoral brasileiro foi alvo de um ataque cibernético durante as eleições legislativas, o que acendeu alertas sobre a fragilidade das defesas digitais estatais (MCTI, 2021).

A ausência de profissionais envolvidos em segurança cibernética, aliada a um arcabouço normativo ainda em desenvolvimento, aprofunda essa vulnerabilidade. De acordo com o Relatório da União Internacional de Telecomunicações (UIT, 2021), o Brasil ocupa posição definida no índice global de cibersegurança, carecendo de políticas integradas de defesa digital que articulem os setores público e privado. A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), embora represente um avanço, ainda não contempla com precisão os desafios impostos pelo ciberterrorismo.

Essa nova ecologia do terrorismo, moldada pelas dinâmicas digitais, exige uma reformulação urgente dos instrumentos de governança internacional em segurança. Como alerta Arquilla e Ronfeldt (1993), estamos lidando com "redes que enfrentam situações", o que requer uma readequação dos sistemas de resposta, de forma a igualar a flexibilidade e a agilidade das estruturas terroristas[3]. A luta contra o terrorismo não pode mais ser travada exclusivamente em campos físicos ou militares; ela ocorre também em espaços de informação, dados e algoritmos.

Diante desse quadro, torna-se necessária a formulação de estratégias que conciliem o imperativo da segurança com a preservação do Estado de Direito. Qualquer política pública que pretenda enfrentar de forma eficaz o terrorismo digital deve ser acompanhado de controles democráticos, de transparência e de respeito às liberdades civis. Como afirma Habermas (1998), os direitos fundamentais não podem ser relativizados nem mesmo diante das ameaças mais graves, pois são eles que sustentam a legitimidade do próprio poder que se propõe a proteger a sociedade. Assim, compreender a complexidade do terrorismo na era digital é condição *sine qua non* para a construção de respostas éticas, jurídicas e práticas, uma vez que as estruturas tradicionais revelam-se manifestamente insuficientes diante desta nova realidade.

[3] O conceito de "Netwar" (guerra em rede), desenvolvido por Arquilla e Ronfeldt, foi fundamental para a compreensão das novas formas de conflito na era da informação, distinguindo-se da "Cyberwar" (guerra cibernética) por focar na manipulação de percepções sociais e na desorganização de redes. Sua relevância para a segurança global continua a ser debatida e refinada. Para mais detalhes, ver: (Arquilla; Ronfeldt, 2001).

3 NORMAS E INSTITUIÇÕES TRADICIONAIS DE SEGURANÇA INTERNACIONAL: DESAFIOS E LIMITAÇÕES

Desde os atentados de 11 de setembro de 2001, a segurança internacional passou a ocupar o centro das agendas políticas globais. A intensificação das ações terroristas e a globalização dos riscos resultaram na criação de mecanismos normativos e institucionais voltados à prevenção e repressão desse fenômeno. No entanto, a crescente migração das ações terroristas para o ambiente digital, bem como o avanço da hiperconectividade[4], têm exposto os limites dessas estruturas tradicionais as quais foram concebidas a partir de um modelo estatal e territorializado de ameaça, o que as torna fundamentalmente despreparadas para a natureza fluida e invisível da ameaça contemporânea, e impõe, como será discutido, profundos desafios jurídicos e filosóficos (Bigo, 2014).

A estratégia da dissuasão (*deterrence*), historicamente eficaz contra ameaças estatais, como no período da Guerra Fria, revela-se inoperante frente a atores não estatais, descentralizados e movidos por motivações ideológicas e religiosas.[5] Segundo Arquilla e Ronfeldt (2001), os grupos terroristas modernos operam em redes flexíveis e adaptáveis, o que os torna resilientes à lógica da dissuasão clássica. A ausência de um "endereço geopolítico" e de uma estrutura hierárquica tradicional impede a responsabilização direta e torna inócuas as ameaças de retaliação ou contenção por força militar convencional.

No plano multilateral, a Organização das Nações Unidas (ONU) tem desempenhado um papel relevante ao articular medidas antiterroristas. A Resolução 1373 (2001) do Conselho de Segurança instituiu obrigações vinculantes aos Estados-membros quanto ao financiamento do terrorismo e à cooperação internacional. Mais recentemente, a Declaração de Delhi (2022), resultado da reunião do Comitê Contra o Terrorismo da ONU, alertou para o uso crescente de

[4] Para uma compreensão mais aprofundada da infraestrutura social e tecnológica que sustenta a "hiperconectividade" e a "sociedade em rede", conceitos fundamentais para a análise do terrorismo digital, ver: (Castells, 2018). Adicionalmente, para uma perspectiva crítica sobre os custos e as implicações éticas das políticas de contraterrorismo, que poderia enriquecer a discussão sobre o equilíbrio entre segurança e direitos fundamentais, sugere-se: (Donohue, 2008).

[5] A teoria da dissuasão, embora influente nas relações internacionais, enfrenta limitações significativas em conflitos assimétricos, onde os atores não estatais podem não possuir "endereço geopolítico" ou responder de forma previsível a ameaças tradicionais. Críticos argumentam que a dependência excessiva da dissuasão pode levar a uma escalada de tensões e a uma corrida armamentista. Para uma análise aprofundada das críticas, ver: (Nye Junior, 2010).

tecnologias emergentes, como drones e criptomoedas, em atividades terroristas, e enfatizou a necessidade de preservar os direitos humanos na luta antiterrorista (UNCTC, 2022). Todavia, tais instrumentos multilaterais enfrentam obstáculos relevantes na implementação prática. A soberania estatal, a assimetria das capacidades tecnológicas e a ausência de uma definição consensual de terrorismo comprometem a efetividade de um regime internacional harmonizado. Como observa Saul (2006), a persistente ambiguidade na definição de terrorismo dificulta acordos de extradição, julgamentos e sanções, favorecendo a seletividade política no uso do termo e comprometendo o princípio da legalidade.

O direito internacional enfrenta um vácuo normativo diante da velocidade com que o terrorismo digital se desenvolve. A atuação de grupos como o Estado Islâmico em plataformas como Telegram e X (antigo Twitter) demonstra como os marcos legais atuais não conseguem acompanhar as transformações tecnológicas. Nesse sentido, Kello (2013) sustenta que os paradigmas clássicos de guerra e segurança tornaram-se obsoletos frente aos ataques cibernéticos e à difusão da violência digital em redes sociais e sistemas criptografados.

O uso da criptografia representa um dos pontos mais controversos desse debate. Por um lado, ela é essencial para proteger dados sensíveis e garantir o sigilo das comunicações; por outro, é frequentemente explorada por grupos terroristas para evitar a detecção e a interceptação estatal. Propostas como a criação de *backdoors* em aplicativos de mensagens são criticadas por comprometerem a segurança global das comunicações. Schneier (2015) adverte que qualquer vulnerabilidade intencional colocada para acesso estatal inevitavelmente será explorada por criminosos e governos autoritários.

No Brasil, a Lei Antiterrorismo (Lei nº 13.260/2016) foi elaborada com base em uma perspectiva ainda centrada no paradigma tradicional do terrorismo, limitando-se a tipificar condutas com ênfase na violência física e deixando de lado a complexidade do terrorismo digital. Autores como Godoy e Oliveira (2020) apontam que a legislação brasileira carece de instrumentos adequados para lidar com a radicalização online, o financiamento via criptoativos e a utilização de *deep web* para fins ilícitos.

A desarticulação entre as legislações nacionais e a ausência de um tratado internacional sistemático sobre terrorismo cibernético revelam a insuficiência das atuais estruturas jurídico-institucionais. Como assinala Guitton (2012), mesmo convenções existentes, como a Convenção de Budapeste sobre crimes cibernéticos, não contemplam com clareza a tipificação

de atos terroristas digitais, o que compromete a responsabilização penal efetiva e a cooperação jurídica internacional.

Outra dimensão crítica é o equilíbrio entre segurança e liberdade. Após os atentados de 2001, diversos Estados expandiram suas capacidades de vigilância, muitas vezes em detrimento das garantias fundamentais. O caso Edward Snowden, ao revelar a amplitude dos programas de espionagem da NSA, evidenciou como o combate ao terrorismo pode ser instrumentalizado para práticas abusivas, colocando em risco direitos como a privacidade, a liberdade de expressão e a presunção de inocência (Greenwald, 2014). Nesse contexto, a legitimidade das instituições de segurança internacional é posta em xeque.

A percepção de seletividade, violação de direitos humanos e ineficiência no enfrentamento das novas modalidades de terrorismo mina a confiança social e internacional. Para Zolo (2010), a segurança global precisa ser pensada a partir de uma lógica cosmopolita e jurídica, que não abdique dos princípios do Estado de Direito em nome de uma racionalidade securitária desmedida. Portanto, é urgente a reformulação das normas e instituições de segurança internacional, não apenas para dar conta das novas modalidades do terrorismo, mas também para reafirmar o compromisso com os valores democráticos. A resposta a esse fenômeno não pode prescindir de uma abordagem interseccional e interdisciplinar, que integre todas as ciências, e que privilegie estratégias preventivas, baseadas em inclusão social, justiça global e educação para os direitos humanos.

4 A ADAPTAÇÃO ÉTICA E EFICAZ: CONCILIANDO SEGURANÇA E DIREITOS FUNDAMENTAIS

A crescente complexidade do terrorismo na era da hiperconectividade digital impõe a necessidade de revisão crítica das abordagens tradicionais de segurança, historicamente centradas em estruturas hierárquicas, estatais e territorializadas. Frente à descentralização das ameaças e à ampliação de seus vetores por meio do ciberespaço, torna-se imperativo pensar em estratégias de enfrentamento que não apenas sejam eficazes do ponto de vista técnico e logístico, mas que se mantenham ancoradas em princípios éticos sólidos e no respeito aos direitos fundamentais.

A eficácia no combate ao terrorismo não pode ser avaliada exclusivamente em função de sua capacidade de neutralizar ameaças, mas deve incluir o critério da legitimidade

democrática. Como afirma Habermas[6] (2007), o Estado democrático de Direito só preserva sua autoridade se o exercício do poder estiver vinculado à legalidade e à deliberação pública. Isso significa que estratégias de segurança não podem ser concebidas em dissonância com os valores que estruturam a própria ordem democrática que pretendem proteger. Caso contrário, incorre-se no paradoxo de combater o terrorismo por meio de práticas que mimetizam sua lógica de exceção e violação.

A radicalização online, por sua vez, mostra-se como um fenômeno que exige mais do que vigilância: requer compreensão social e política. A radicalização não pode ser reduzida a uma patologia individual, pois decorre frequentemente de contextos de exclusão, discriminação e ressentimento. A resposta estatal, portanto, não deve se limitar à repressão, mas incluir políticas preventivas voltadas à inclusão, à educação crítica e à redução de vulnerabilidades sociais que tornam indivíduos suscetíveis ao discurso extremista.

A coleta e análise de dados no ambiente digital configuram uma das áreas mais sensíveis no equilíbrio entre segurança e privacidade. O escândalo revelado por Edward Snowden em 2013 demonstrou o grau de intrusão das agências de inteligência dos Estados Unidos, especialmente a NSA, nos dados privados de cidadãos em todo o mundo (Greenwald, 2014). A vigilância em massa, longe de se mostrar eficaz, compromete a confiança pública nas instituições e cria um clima de suspeição generalizada que debilita os laços democráticos. Como enfatiza Zuboff (2019), a lógica do "capitalismo de vigilância" transforma a privacidade em uma mercadoria, favorecendo o controle em detrimento da autonomia cidadã.

No Brasil, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabelecem diretrizes importantes para a preservação de direitos digitais. Ambas as normas são referências no contexto latino-americano por estabelecerem parâmetros claros para a responsabilização de agentes públicos e privados quanto ao uso de dados pessoais, além de promoverem a neutralidade da rede e a liberdade de expressão. Conforme destaca Doneda (2021), essas legislações demonstram que é possível articular avanços tecnológicos com salvaguardas institucionais robustas, embora o desafio esteja na constante atualização desses marcos frente à inovação acelerada. Entretanto, o

[6] A teoria do discurso de Jürgen Habermas, especialmente em "Direito e Democracia", estabelece uma relação intrínseca entre o Estado de Direito e a democracia, argumentando que a legitimidade do poder reside na deliberação pública e no respeito aos direitos humanos (Habermas, 2007).

arcabouço normativo precisa ser continuamente aprimorado diante das metamorfoses do fenômeno terrorista digital. A resposta legal deve ser flexível o suficiente para acompanhar novas modalidades de ameaça, mas sem se tornar um instrumento de exceção permanente. Como bem observa Agamben (2004), a proliferação de dispositivos jurídicos de exceção[7], muitas vezes justificados pela urgência da segurança, compromete a fronteira entre legalidade e arbitrariedade, corroendo o próprio princípio da cidadania.

O desafio ético central consiste em combater a violência sem sacrificar os fundamentos do Direito. A Organização das Nações Unidas, por meio de sua Estratégia Global de Combate ao Terrorismo, reitera que todas as ações antiterroristas devem respeitar os direitos humanos e as liberdades fundamentais (United Nations, 2020). Isso implica em garantir o devido processo legal, evitar práticas como tortura, detenções arbitrárias e vigilância indiscriminada, além de manter a independência do Judiciário e a transparência na formulação das políticas de segurança.

A regulação das plataformas digitais, onde frequentemente circulam discursos de ódio e propaganda extremista, representa um dos maiores dilemas do presente. A tentativa de impor restrições ao conteúdo deve ser feita com extremo cuidado para não incorrer em censura ou discriminação injustificada. A Declaração de Delhi sobre Liberdade de Expressão (UNESCO, 2021) aponta que a moderação de conteúdo por empresas privadas deve ser acompanhada de critérios legais claros, mecanismos de apelação e supervisão independente, sob pena de se criar zonas cinzentas de repressão não estatal.

A participação da sociedade civil é fundamental para garantir a legitimidade das medidas antiterroristas. Organizações não governamentais, defensores de direitos humanos e especialistas técnicos devem ser integrados ao debate sobre regulação, vigilância e proteção de dados. Como observa Morozov (2011), a governança digital não pode ser deixada exclusivamente nas mãos de governos e corporações, sob risco de se instituir um novo autoritarismo algorítmico travestido de segurança. O combate eficaz ao terrorismo exige, portanto, um novo paradigma de inteligência. Ao invés de priorizar apenas a coleta massiva de informações, é necessário investir em capacidades analíticas, interoperabilidade entre agências

[7] O conceito de "estado de exceção" de Giorgio Agamben, desenvolvido a partir de Carl Schmitt, explora como a suspensão temporária da lei em situações de crise pode se tornar uma prática permanente, erodindo as garantias jurídicas e transformando a exceção em regra. (AGAMBEN, 2004).

e respeito aos limites legais. Como defende Bauman (2016), a segurança não deve ser concebida como um fim absoluto, mas como um valor a ser equilibrado com outros bens igualmente importantes, como a liberdade e a dignidade humana.

É preciso reconhecer que a resposta antiterrorista não pode ser militarizada em demasia, sob pena de transformar os espaços civis em zonas de exceção. A militarização da segurança pública, como alerta Silva (2022), tende a reproduzir lógicas de guerra que são incompatíveis com a proteção de direitos, especialmente em contextos democráticos fragilizados. O terrorismo deve ser enfrentado com instrumentos do Estado de Direito, e não com a suspensão de seus próprios mecanismos garantidores.

A proteção dos dados pessoais e o fortalecimento da cibersegurança devem ser acompanhados de mecanismos democráticos de fiscalização. A criação de autoridades independentes de proteção de dados, com poder de sanção e transparência em suas deliberações, é essencial para assegurar que medidas excepcionais não se convertam em políticas permanentes de vigilância e controle.

É igualmente urgente investir na alfabetização digital da população, promovendo uma cidadania ativa e consciente dos riscos e direitos no ambiente online. A educação para o uso crítico das redes é um antídoto preventivo à manipulação informacional e ao recrutamento por narrativas extremistas. A inclusão digital, acompanhada de formação ética e crítica, pode ser uma ferramenta poderosa de resistência à radicalização.

Em última instância, a adaptação ética das políticas de segurança internacional passa por reconhecer que não há segurança duradoura sem justiça, e não há justiça sem direitos. Isso implica uma busca contínua pela justiça global, combatendo as desigualdades e exclusões sociais que, como vetores de ressentimento, podem ser exploradas por narrativas extremistas e se tornar solo fértil para a radicalização. A eficácia operacional, portanto, não pode obscurecer a centralidade dos princípios jurídicos e democráticos que organizam a convivência moderna. Qualquer política pública que busque enfrentar o terrorismo deve ser capaz de reforçar esses fundamentos, e não de corroê-los sob o pretexto da urgência.

O futuro do combate ao terrorismo na era digital dependerá da capacidade dos Estados e das sociedades em construir respostas que conjuguem tecnologia, direitos humanos e governança democrática. Trata-se de um desafio complexo, mas inadiável. O preço de

negligenciá-lo pode ser alto: uma sociedade vigiada, desconfiada e cada vez mais distante dos ideais que pretende defender.

5 ESTRATÉGIAS PARA O COMBATE AO TERRORISMO DIGITAL

A crescente digitalização da sociedade ampliou o alcance e a complexidade das ameaças terroristas, exigindo uma resposta estratégica multifacetada. O enfrentamento do terrorismo na era da hiperconectividade deve articular dimensões técnicas, humanas, institucionais e jurídicas, em um esforço que transcenda fronteiras nacionais e que respeite os pilares fundamentais do Estado de Direito. Essa abordagem deve, necessariamente, equilibrar a eficácia das ações de segurança com a proteção das liberdades civis, num campo em que os excessos podem corroer os próprios valores democráticos que se pretende proteger (Cole, 2003).

No âmbito das medidas técnicas, é essencial o desenvolvimento e o aprimoramento de ferramentas que garantam tanto a segurança digital quanto a privacidade dos usuários legítimos. Tecnologias como criptografia de ponta, autenticação multifatorial e análise preditiva de comportamento são fundamentais para impedir acessos indevidos e prevenir ataques. Entretanto, o uso dessas tecnologias deve observar parâmetros éticos estritos, para que não se transformem em instrumentos de vigilância massiva, como alerta Zuboff (2019), ao denunciar o risco de uma sociedade orientada pela lógica da "vigilância comportamental".

O desafio da proteção cibernética se intensifica quando consideramos a natureza descentralizada do terrorismo digital. Grupos extremistas exploram brechas na legislação e na infraestrutura digital para se comunicarem de forma criptografada, muitas vezes imunes à ação estatal. Como observa Schneier (2015), a criptografia é uma "espada de dois gumes": ao mesmo tempo em que protege cidadãos comuns, pode blindar comunicações criminosas. Nesse sentido, a criação de 'backdoors' ou vulnerabilidades intencionais em sistemas criptográficos deve ser veementemente desaconselhada como estratégia antiterrorista. Tais 'portas dos fundos' comprometem irremediavelmente a segurança global das comunicações para todos os usuários e, uma vez criadas, se tornam alvos inevitáveis para criminosos e atores estatais mal-intencionados, minando a confiança e a integridade da infraestrutura digital. Assim, a regulação do uso de criptografia exige uma abordagem calibrada, que preserve os direitos à privacidade sem deixar espaços impunes à criminalidade transnacional.

Nesse cenário, a capacitação humana torna-se um dos pilares mais estratégicos. Há um déficit global de especialistas em cibersegurança, e o Brasil não é exceção. Segundo relatório da (ISC)², o país enfrenta uma carência superior a 400 mil profissionais da área (ISC², 2023). A formação de agentes públicos, analistas de inteligência, promotores e juízes deve ir além da dimensão técnica, incorporando reflexões jurídicas, filosóficas e sociais. Como destaca Tanguay (2020), a segurança digital não é apenas uma questão de ferramentas, mas de princípios e valores que devem ser compreendidos por aqueles que operam o sistema.

A cooperação institucional entre agências públicas e a articulação com o setor privado é indispensável. O terrorismo digital opera em redes fragmentadas e transfronteiriças; sua contenção exige uma resposta igualmente conectada. Protocolos de cooperação entre polícia, serviços de inteligência, agências reguladoras, empresas de tecnologia e instituições financeiras devem ser estabelecidos, com salvaguardas legais adequadas. A experiência europeia, em especial o modelo da Europol e da sua Unidade de Referência na Internet (IRU), mostra que a articulação multinível pode ter efeitos concretos na remoção de conteúdos extremistas e na antecipação de ataques (EUROPOL, 2022).

No contexto brasileiro[8], ainda, a criação de uma agência nacional de segurança cibernética com foco no combate ao terrorismo digital se revela uma medida urgente e alinhada às melhores práticas internacionais. Embora o país conte com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), ainda não possui uma instância civil dedicada exclusivamente ao enfrentamento dessa modalidade de ameaça. A proposta de uma agência com atribuições específicas nesse campo encontra paralelo em países como Israel e Reino Unido, que centralizaram as respostas estatais em organismos altamente especializados e autônomos (Clarke; Knake, 2012). Ao adotar um modelo que integra coordenação estratégica, produção de inteligência e fomento à cooperação internacional, o Brasil não só fortalece sua própria defesa digital, mas também se posiciona como um ator relevante na construção de um regime global de cibersegurança mais robusto, aprendendo e contribuindo com as experiências internacionais. Tal agência deveria desempenhar funções de

[8] O Brasil já possui uma Estratégia Nacional de Cibersegurança (E-Ciber), estabelecida em 2020, que busca uma visão integrada e centralizada da cibersegurança. No entanto, relatórios indicam que as tentativas passadas foram "fragmentadas e ad-hoc", e que ainda há "considerável ambiguidade" na implementação desse modelo centralizado, além de um déficit de profissionais na área. Para uma análise dos desafios e da evolução da cibersegurança no Brasil, ver: (Instituto Igarapé, 2021).

coordenação estratégica, produção de inteligência, normatização técnica e fomento à cooperação internacional. Sua atuação, contudo, não poderia prescindir de mecanismos robustos de controle externo e transparência. Conforme sustenta Mendes (2015), a centralização do poder estatal na área de segurança deve ser acompanhada de contrapesos institucionais eficazes, sob pena de abrir caminho para práticas autoritárias em nome da segurança.

A participação da sociedade civil é fundamental nesse processo. Organizações não governamentais, grupos de direitos humanos e centros acadêmicos têm papel relevante na fiscalização das políticas antiterroristas, assegurando que elas não extrapolem os limites do Estado Democrático de Direito. Como alerta Dworkin (2006), a legitimidade das instituições democráticas repousa na sua capacidade de garantir liberdades mesmo diante de ameaças graves. Nesse sentido, os mecanismos de *accountability* devem ser fortalecidos, com canais efetivos de denúncia, avaliação e correção das ações estatais.

O setor privado, particularmente as grandes plataformas digitais, possui responsabilidade direta no combate ao terrorismo online. Empresas como Google, Meta e X já possuem políticas de moderação de conteúdo e sistemas de detecção automatizada de discurso extremista, mas sua eficácia ainda é limitada. Como aponta Citron (2018), essas corporações devem adotar políticas mais claras e auditáveis, submetidas ao escrutínio público, com garantias contra censura arbitrária e respeito à liberdade de expressão.

A cooperação internacional é outro vetor indispensável. O terrorismo digital não reconhece fronteiras, e a fragmentação legislativa entre os países gera brechas exploradas por grupos extremistas. Instrumentos como a Convenção de Budapeste sobre o Cibercrime (2001) e a Declaração de Delhi da ONU (2022) apontam caminhos para a harmonização legislativa e a intensificação da assistência jurídica mútua. O Brasil, como signatário desses esforços, deve avançar na adaptação de seu ordenamento jurídico, criando normas que dialoguem com os padrões internacionais de direitos humanos e proteção de dados.

A atuação coordenada de organismos internacionais, como a ONU, a OEA e a Interpol, também deve ser fortalecida. Iniciativas como o UN Counter-Terrorism Centre e o Tech Against Terrorism mostram que é possível estabelecer redes globais de cooperação técnica e normativa, desde que fundadas na transparência e no respeito às soberanias nacionais. No entanto, é preciso cuidado com a sobreposição de competências e a possível imposição de

agendas unilaterais, que possam comprometer a autodeterminação dos Estados periféricos (Santos, 2002).

Por fim, o combate ao terrorismo digital deve ser orientado por uma ética da responsabilidade. Como defendia Max Weber (2006), a responsabilidade no exercício do poder deve ser acompanhada de prudência, proporcionalidade e consciência das consequências. Weber estabelece uma distinção crucial entre a ética da convicção, que pauta a ação por princípios morais absolutos e inegociáveis, e a ética da responsabilidade, que exige a ponderação das consequências previsíveis das decisões. No contexto do exercício do poder, Weber argumenta que a ética da responsabilidade é fundamental. Isso implica que os detentores de poder, em qualquer esfera – seja política, administrativa ou outra –, devem avaliar meticulosamente as implicações de suas ações, visando minimizar os impactos negativos e maximizar os benefícios para a sociedade. A combinação da ética da responsabilidade com a prudência, a proporcionalidade e a plena consciência das consequências é, para Weber, essencial para um exercício legítimo e eficaz do poder, capaz de prevenir abusos e promover o bem-estar social. O imperativo moral de proteger vidas não pode ser instrumentalizado como pretexto para práticas arbitrárias ou discriminatórias. É nesse ponto que a interseção entre as ciências oferece instrumentos para uma abordagem reflexiva, orientada por princípios de justiça, equidade e dignidade humana.

Em síntese, as estratégias de combate ao terrorismo digital devem ser guiadas por um modelo holístico, que articule inovação tecnológica, formação ética, normatização equilibrada e cooperação efetiva. O sucesso dessa empreitada dependerá da capacidade das sociedades democráticas de construírem respostas eficazes à ameaça, sem perder de vista os valores que pretendem defender. O desafio é, portanto, não apenas técnico, mas sobretudo político, jurídico e moral.

6 CONSIDERAÇÕES FINAIS

O presente estudo partiu da constatação de que o terrorismo contemporâneo, inserido no contexto da hiperconectividade digital, representa um fenômeno qualitativamente distinto em relação às formas clássicas de violência política. A partir da problematização central - como as normas, instituições e estratégias tradicionais de segurança internacional podem responder, de modo ético e eficaz, à difusão e atomização do terrorismo digital sem comprometer os

fundamentos do Estado de Direito, procurou-se construir uma análise crítica e multidisciplinar, ancorada nos campos do Direito, da Filosofia Política e das Relações Internacionais.

A investigação revelou que a emergência de novas tecnologias, como a criptografia de ponta, as redes descentralizadas e os algoritmos de automação comunicacional, não apenas transformou os meios de ação dos grupos terroristas, mas também desafiou os paradigmas normativos e operacionais das políticas de segurança global. O terrorismo já não opera apenas como insurgência armada ou sabotagem física, mas como uma guerra simbólica, informacional e psicológica, que manipula vulnerabilidades sistêmicas do ambiente digital globalizado.

Nesse sentido, a hiperconectividade atua como acelerador da radicalização individual, potencializa o alcance das narrativas extremistas e dificulta a rastreabilidade de ações coordenadas. Diante desse quadro, estratégias tradicionais de dissuasão estatal, ancoradas na previsibilidade de atores e fronteiras geopolíticas estáveis, mostram-se anacrônicas. A fluidez do terrorismo em rede exige, portanto, um redimensionamento teórico e prático das respostas institucionais. Entretanto, essa adaptação não pode se dar à custa dos princípios basilares do Estado de Direito, das liberdades individuais e da dignidade humana, sob pena de se esvaziar a própria legitimidade da resposta estatal ao terrorismo digital.

A tensão entre segurança e liberdade é real, mas a resposta normativa e política deve ser orientada por um imperativo ético: a proteção da vida e da ordem pública não pode legitimar práticas de vigilância indiscriminada, censura prévia ou exceção permanente. A experiência histórica e os casos recentes - como o de Edward Snowden - ilustram os riscos de erosão democrática sob o pretexto da proteção. Por isso, a resposta ao terrorismo hiperconectado deve ser compreendida como um exercício de governança global responsável, que articule tecnologia, direito e democracia. A criação de marcos regulatórios para as plataformas digitais, a institucionalização de mecanismos transparentes de controle das ações estatais e a defesa da criptografia como direito à privacidade compõem um tripé normativo indispensável para o equilíbrio entre segurança e liberdade.

Ademais, a efetividade das políticas antiterroristas dependerá de sua capacidade de construir redes de cooperação internacional e interinstitucional. A harmonização legislativa transnacional, a capacitação contínua de profissionais em cibersegurança, o investimento em inteligência estratégica e a articulação entre setor público, empresas de tecnologia e sociedade

civil organizada são estratégias indispensáveis para prevenir e mitigar ataques sem abrir mão da legitimidade democrática.

O papel da educação crítica e da alfabetização digital também merece destaque, uma vez que a formação cidadã e o fortalecimento da resiliência social contra discursos de ódio e manipulação ideológica representam barreiras fundamentais à expansão das agendas extremistas. O terrorismo não se combate apenas com tecnologia, mas com cultura democrática e cidadania ativa.

Em síntese, este artigo defende que o enfrentamento ao terrorismo na era da hiperconectividade digital deve se pautar por uma lógica de proteção ampliada, que reconhece a complexidade das ameaças e, ao mesmo tempo, preserva a dignidade humana como limite intransponível da ação estatal. Não se trata de escolher entre liberdade ou segurança, mas de construir uma arquitetura jurídica e institucional que garanta ambas, de modo sinérgico e sustentável.

Conclui-se, portanto, que o verdadeiro desafio contemporâneo reside em afirmar os valores democráticos precisamente onde eles são mais testados: nos momentos de crise, medo e incerteza. A resposta ética ao terrorismo digital não pode ser a suspensão da liberdade, mas a reafirmação incondicional de sua centralidade como princípio orientador da ordem internacional justa e legítima.

REFERÊNCIAS

AGAMBEN, G. **Estado de exceção**. São Paulo: Boitempo, 2004.

ARQUILLA, J.; RONFELDT, D. **Networks and Netwars:** The Future of Terror, Crime, and Militancy. Santa Monica: RAND Corporation, 1993.

ARQUILLA, J.; RONFELDT, D. **Networks and Netwars:** The Future of Terror, Crime, and Militancy. Santa Monica: RAND Corporation, 2001.

BAUMAN, Z. **Vigilância líquida**. Rio de Janeiro: Zahar, 2016.

BIGO, D. Security, Freedom and Accountability: Linking Security Policies to Human Rights. *In:* KRAUSE, K.; WILLIAMS, M. (org.). **Critical Security Studies.** London: Routledge, 2014. p. 33- 52.

BOCCHINO, F. Criptografia e Comunicação Segura entre Terroristas: Desafios e Respostas na Segurança Internacional. **Relações Exteriores**. 2025. Disponível em: https://relacoesexteriores.com.br/criptografia-comunicacao-terroristas/. Acesso em: 29 jul. 2025.

BRASIL. Lei nº 12.965, de 23 abr. 2014. Marco Civil da Internet. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.260, de 16 mar. 2016. Dispõe sobre o crime de terrorismo. **Diário Oficial da União**, Brasília, DF, 17 mar. 2016.

BRASIL. Lei nº 13.709, de 14 ago. 2018. Lei Geral de Proteção de Dados Pessoais. **Diário Oficial da União**, Brasília, DF, 15 ago. 2018.

CASTELLS, M. **A sociedade em rede.** 15. ed. São Paulo: Paz e Terra, 2018.

CITRON, D. K. Extremist Speech, Compelled Conformity, and Censorship Creep. **Notre Dame Law Review**, Notre Dame, v. 93, n. 3, p. 1011-1049, 2018.

COLE, D. **Enemy aliens:** Double standards and constitutional freedoms in the war on terrorism. New York: The New Press, 2003.

DONEDA, D. Proteção de dados pessoais: a evolução histórica e legislativa no Brasil. **Revista Brasileira de Políticas Públicas**, v. 11, n. 1, 2021.

DONOHUE, L. K. **The cost of counterterrorism:** power, politics, and liberty. Cambridge: Cambridge University Press, 2008.

DUNN CAVELTY, M. **Cyber-Security and Threat Politics:** US Efforts to Secure the Information Age. New York: Routledge, 2013.

DWORKIN, R. **Is democracy possible here?** Principles for a new political debate. Princeton: Princeton University Press, 2006.

EUROPOL. **Internet Referral Unit annual report 2021**. Haia: Europol, 2022. Disponível em: https://www.europol.europa.eu. Acesso em: 10 jul. 2025.

GODOY, A. S.; OLIVEIRA, T. C. de. Terrorismo e o uso da internet: desafios legais e estratégias de enfrentamento no Brasil. **Revista Brasileira de Políticas Públicas**, v. 10, n. 2, p. 38-56, 2020.

GREENWALD, G. **Sem lugar para se esconder:** Edward Snowden, a NSA e a espionagem do governo americano. São Paulo: Companhia das Letras, 2014.

GUITTON, C. Cyber insecurity as a national threat: overreaction from Germany, France and the UK? **European Security**, v. 21, n. 1, p. 63-81, 2012.

HABERMAS, J. **Direito e democracia:** entre facticidade e validade. Rio de Janeiro: Tempo Brasileiro, 1998. v. I.

HABERMAS, J. **Direito e democracia:** entre facticidade e validade. Rio de Janeiro: Tempo Brasileiro, 2007.

INSTITUTO IGARAPÉ. **Cybersecurity in Brazil.** Rio de Janeiro: Instituto Igarapé, 2021.

ISC. **Cybersecurity Workforce Study 2023**. Alexandria: ISC², 2023.

KELLO, L. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. **International Security**, v. 38, n. 2, p. 7-40, 2013.

KHOSROKHAVAR, F. **Radicalisation.** Paris: Maison des Sciences de l'Homme, 2018.

KNAKE, R. K. **Cyber war:** The next threat to national security and what to do about it. New York: HarperCollins, 2012.

MACDONALD, S.; WHITTAKER, D. **Online Radicalisation:** What We Know. Migration and Home Affairs, European Commission, 2019.

MENDES, C. **Controle de constitucionalidade e democracia.** São Paulo: Saraiva, 2015.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES (MCTI). Relatório de Ocorrências de Incidentes Cibernéticos no Brasil – 2021. Brasília: CGSI, 2021.

MOROZOV, E. **The Net Delusion:** The Dark Side of Internet Freedom. New York: PublicAffairs, 2011.

NASCIMENTO, A.; AMARAL, C. Extremismo e redes digitais no Brasil: cartografias da radicalização. **Revista Brasileira de Segurança Pública**, São Paulo, v. 16, n. 1, p. 105-126, 2022.

NEUMANN, P. R. **Radicalized:** New Jihadists and the Threat to the West. London: I.B. Tauris, 2013.

NYE JUNIOR, J. S. Deterrence and Counterterrorism. **International Security**, v. 35, n. 1, p. 14-32, 2010.

ROY, O. The Myth of Grass-Roots Terrorism: Why Osama bin Laden Still Matters. **Foreign Affairs**, v. 87, n. 3, p. 196-206, 2008.

SAGEMAN, M. **Leaderless Jihad:** Terror Networks in the Twenty-First Century. Philadelphia: University of Pennsylvania Press, 2008.

SANTOS, B. de S. **Crítica da razão indolente:** contra o desperdício da experiência. São Paulo: Cortez, 2002.

SAUL, B. **Defining Terrorism in International Law.** Oxford: Oxford University Press, 2006.

SCHNEIER, B. **Data and Goliath:** The hidden battles to collect your data and control your world. New York: W. W. Norton & Company, 2015.

SILVA, F. Segurança pública, militarização e Estado de Direito. **Revista Brasileira de Ciências Criminais**, v. 30, n. 175, 2022.

TANGUAY, D. *Ethics and cybersecurity: A handbook*. Montreal: IRI, 2020.

UNESCO. Delhi Declaration on Freedom of Expression and the Internet. Paris: UNESCO, 2021.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT). Global Cybersecurity Index (GCI) 2021. Geneva: ITU, 2021.

UNITED NATIONS COUNTER-TERRORISM COMMITTEE (UNCTC). Delhi Declaration on Countering the Use of New and Emerging Technologies for Terrorist Purposes. United Nations, 2022.

UNITED NATIONS. UN Global Counter-Terrorism Strategy. New York: United Nations, 2020.

WEBER, M. **A política como vocação.** Tradução de Waldir Rego. São Paulo: Cultrix, 2006.

ZOLO, D. **Cosmópolis:** perspectivas do governo mundial. São Paulo: Martins Fontes, 2010.

ZUBOFF, S. **The Age of Surveillance Capitalism.** New York: PublicAffairs, 2019.

Sobre a autoria

Douglas Aparecido Bueno
Doutor em Filosofia (PUC-SP). Professor do Programa de Pós-Graduação em Filosofia - Mestrado da Universidade Federal de Rondônia.
douglas.bueno@unir.br

Contribuição de autoria
Douglas Aparecido Bueno: concepção, coleta de dados, análise de dados, elaboração do manuscrito, redação, discussão dos resultados.

Financiamento (se houver)
Não se aplica.

Consentimento de Uso de Imagem
Não se aplica.