

**FUNDAÇÃO EDUCACIONAL MACHADO DE ASSIS
FACULDADES INTEGRADAS MACHADO DE ASSIS
CURSO DE DIREITO**

SARA LETÍCIA DE LIMA

**(NEO)TERRORISMO: AMEAÇAS CIBERNÉTICAS E A
RACIONALIDADE DA LEI PENAL
TRABALHO DE CURSO**

Santa Rosa
2022

SARA LETÍCIA DE LIMA

**(NEO)TERRORISMO: AMEAÇAS CIBERNÉTICAS E A RACIONALIDADE DA
LEI PENAL
TRABALHO DE CURSO**

Monografia apresentada às Faculdades Integradas Machado de Assis, como requisito parcial para obtenção do Título de Bacharel em Direito.

Orientador(a): Professor Cláudio Rogério Sousa Lira.

Santa Rosa
2022

SARA LETÍCIA DE LIMA


**(NEO)TERRORISMO: AMEAÇAS CIBERNÉTICAS E A RACIONALIDADE DA LEI
PENAL
TRABALHO DE CURSO**

Monografia apresentada às Faculdades Integradas Machado de Assis, como requisito parcial para obtenção do Título de Bacharel em Direito.

Banca Examinadora



Prof. Dr. Cláudio Rogério Sousa Lira – Orientador(a)



Prof. Ms. Rafael Lago Salapata



Prof. Esp. William Dal Bosco Garcez Alves

Santa Rosa, 06 de julho de 2022.

DEDICATÓRIA

Dedico esta monografia a minha família e amigos, em especial aos meus pais Robinson de Lima e Sandra de Almeida.

AGRADECIMENTOS

Inicialmente, agradeço a Deus por, ao longo deste processo desgastante e complexo, me ter feito ver o caminho, nos momentos em que pensei em desistir.

Aos meus pais Robinson e Sandra, sem os quais nada disso seria possível, devo a vida a vocês e espero um dia poder lhes retribuir todos os sacrifícios realizados ao longo de toda a minha existência, principalmente no decorrer destes 5 anos de graduação, para que eu pudesse realizar o sonho de me tornar bacharel em direito.

Agradeço ainda aos meus amigos e familiares que ao longo dessa etapa me encorajaram e me apoiaram, em especial as minhas amigas/irmãs Jéssica Liara, Gabriela Bamberg e Maethe Matos, as quais trilharam comigo essa jornada inesquecível, tornando-a uma das melhores fazes da minha vida.

Deixo também um agradecimento especial aos meus professores, em particular ao meu orientador Cláudio Rogério Sousa Lira, pois sem esse não seria possível esta monografia.

Só se vive o propósito quem suporta
o processo.

Marcos Cruz Santos.

RESUMO

O presente tema trata das ações radicais de grupos terroristas que atinge as multidões civis e do crescimento das ameaças cibernéticas com enfoque no processo de racionalidade da lei penal. A delimitação temática estudará acerca do crescimento das ações radicais de grupos terroristas, os efeitos diretos e indiretos do (neo)terrorismo e a política criminal do processo de racionalidade da lei penal do Brasil como possível resposta jurídica à expansão dos crimes cibernéticos. A problemática questiona em que medida o Direito Penal se revela em resposta Jurídica do Estado na prevenção e repressão à expansão dos grupos terroristas e ao aumento das formas de ameaças cibernéticas? O objetivo geral do presente trabalho é analisar a expansão dos grupos terroristas, a utilização de ameaças cibernéticas e a disseminação de novos métodos para a expansão do (neo)terrorismo, a fim de verificar a racionalidade da lei penal como resposta jurídica do Estado. Concebe-se que este assunto possui expressivo potencial para ensejar debates a respeito das novas ameaças cibernéticas e à utilização da mesma para a realização de uma nova forma de ataque terrorista, uma vez que a internet não permanece mais apenas como meio de recrutamento para novos membros, mas, também, como forma de expandir seus atos terroristas. Atualmente a temática não é abordada por inúmeros autores, no entanto Baptista, Raposo, Wilkinson, Witcker e Woslozyn, são os principais autores que abordam a temática. No presente trabalho, a metodologia consiste no estudo das práticas do saber e das práticas de exercício do saber, tendentes ao aperfeiçoamento dos conhecimentos humanos (BITTAR, 2015, p.44). A estruturação do trabalho foi dividida em três capítulos, sendo o primeiro capítulo o contexto histórico e a conceituação de terrorismo, já o segundo capítulo discorre quanto a expansão do (neo)terrorismo e seu “*modus operandi*”, por fim, o último capítulo apresenta os fundamentos doutrinários e legislativos sobre as penalidades acerca dos atos terroristas. A metodologia utilizada no trabalho tem natureza teórica, objetivando fins descritivos, com o tratamento de dados de forma qualitativa, utilizando procedimentos técnicos bibliográficos e documentais, com a contemplações em fontes secundárias de pesquisa bibliográfica e como método de abordagem o hipotético-dedutivo. Ao cabo, se verificou-se a carência do Código Penal brasileiro em relação ao crime de terrorismo, a escassez de dispositivos com o intuito de prevenir e reprimir os atos terroristas e a necessidade regulamentar novos dispositivos que tratem sobre o terrorismo.

Palavras-chave: (neo)terrorismo - ataques terroristas - ameaças cibernéticas - grupos terroristas.

ABSTRACT

The present theme deals with the radical actions of terrorist groups that affect civilian crowds and the growth of cyber threats with a focus on the rationality process of criminal law. The thematic delimitation will study about the growth of radical actions of terrorist groups, the direct and indirect effects of (neo)terrorism and the criminal policy of the rationality process of Brazilian criminal law as a possible legal response to the expansion of cyber crimes. The problem questions the extent to which Criminal Law reveals itself in the State's legal response in preventing and repressing the expansion of terrorist groups and the increase in forms of cyber threats? The present work seeks to analyze the expansion of terrorist groups, the use of cyber threats and the dissemination of new methods for the expansion of (neo)terrorism, in order to verify the rationality of criminal law as a legal response of the State. It is conceived that this subject has significant potential to give rise to debates about the new cyber threats and the use of it to carry out a new form of terrorist attack, since the internet no longer remains only as a means of recruiting new members, but also as a way to expand their terrorist acts. Currently, the theme is not addressed by numerous authors, however Baptista, Raposo, Wilkinson, Witcker and Woslozyn are the main authors who approach the theme. In the present work, the methodology consists of the study of knowledge practices and practices of exercising knowledge, aimed at improving human knowledge (BITTAR, 2015, p.44). The structuring of the work was divided into three chapters, the first chapter being the historical context and the concept of terrorism, the second chapter discusses the expansion of (neo)terrorism and its "modus operandi", finally, the last chapter presents the doctrinal and legislative foundations on penalties for terrorist acts. The methodology used in the work is theoretical in nature, aiming at descriptive purposes, with qualitative data processing, using bibliographic and documentary technical procedures, with consideration of secondary sources of bibliographic research and the hypothetical-deductive approach method. In the end, the lack of the Brazilian Penal Code in relation to the crime of terrorism, the scarcity of devices to prevent and repress terrorist acts and the need to regulate new devices that address terrorism were verified.

Keywords: (neo)terrorism - terrorist attacks - cyber threats - terrorist groups.

LISTA DE ABREVIÇÕES, SIGLAS E SÍMBOLOS

Nº - Número

p. – Página

§ - Parágrafo

d. C –Depois de Cristo

ANPD – Autoridade Nacional de Proteção de Dados

ART – Artigo

CF – Constituição Federal

CP – Código Penal

DAT – Departamento Antiterrorismo da Polícia Federal

DPF – Departamento da Polícia Federal

EI – Estado Islâmico

EUA – Estados Unidos da América

ISIS – Estado Islâmico

LGPD – Lei Geral de Proteção de Dados

MPF – Ministério Público Federal

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte

SUMÁRIO

INTRODUÇÃO	10
1 O TERRORISMO E O (NEO)TERRORISMO	13
1.1 CONCEITO DE TERRORISMO.....	13
1.2 SURGIMENTO DO TERRORISMO E DO (NEO)TERRORISMO	16
1.3 DISTINÇÕES NECESSÁRIAS.....	18
2 A EXPANSÃO DO (NEO)TERRORISMO E SEU “MODUS OPERANDI”	22
2.2 <i>MODUS OPERANDI</i> DO (NEO)TERRORISMO E TERRORISMO CIBERNÉTICO E SUAS FINALIDADES	24
2.3 OS PRINCIPAIS GRUPOS TERRORISTAS DA ATUALIDADE	29
3 FUNDAMENTOS DOUTRINÁRIOS E LEGISLATIVOS SOBRE AS PENALIDADES ACERCA DOS ATOS TERRORISTAS	35
3.1 ANÁLISE DA LEI 13.260/2016 – LEI ANTITERRORISMO.....	37
3.2 CARÊNCIA DO CÓDIGO PENAL EM RELAÇÃO AO CRIME DE (NEO)TERRORISMO	44
CONCLUSÃO	48
REFERÊNCIAS	51

INTRODUÇÃO

O tema em questão é o (neo)terrorismo: ameaças cibernéticas e a racionalidade da lei penal, cuja delimitação estuda o crescimento das ações radicais de grupos terroristas, os efeitos diretos e indiretos do (neo)terrorismo e a política criminal do processo de racionalidade da lei penal do Brasil como possível resposta jurídica à expansão dos crimes cibernéticos.

A problemática questiona em que medida o Direito Penal se revela em resposta Jurídica do Estado na prevenção e repressão à expansão dos grupos terroristas e ao aumento das formas de ameaças cibernéticas?

Como maneira de obter as respostas para a problemática acima arguida, o desenvolvimento da pesquisa será traçado com base nas três hipóteses de desenvolvimento abaixo mencionadas.

A primeira sustenta que a racionalidade da lei penal não sofre com a expansão do (neo)terrorismo, tampouco com as novas ameaças cibernéticas, visto que possui como disciplinador da matéria a Lei nº 13.260 de 2016, denominada de Lei Antiterrorismo. A segunda parte da premissa de que a lei penal tem sua racionalidade afetada de forma direta, devido ao crescimento de diversos meios para o alastramento dos ataques terroristas, principalmente, ligados a ameaças cibernéticas, tendo em vista escassez de dispositivos reguladores de tal conteúdo. A terceira e última hipótese é baseada na assertiva de que a atual política criminal se mostra uma eficaz forma de resposta jurídica para prevenir e reprimir as novas práticas terroristas cibernéticas.

Em relação ao objetivo geral, o presente trabalho busca analisar a expansão dos grupos terroristas, a utilização de ameaças cibernéticas e a disseminação de novos métodos para a expansão do (neo)terrorismo, a fim de verificar a racionalidade da lei penal como resposta jurídica do Estado.

No que diz respeito aos objetivos específicos a pesquisa será conduzida a partir da análise da expansão dos grupos terroristas, a utilização de ameaças cibernéticas e a disseminação de novos métodos para a expansão do (neo)terrorismo, a fim de verificar a racionalidade da lei penal como resposta

jurídica do Estado. Ademais, busca estudar o “Modus Operandi” do Terrorismo Cibernético, bem como os objetivos dos principais grupos que disseminam essas práticas. Outra razão pela qual a presente monografia está sendo realizada é para estudar os fundamentos doutrinários e legislativos sobre as penalidades acerca dos atos terroristas, com ênfase nas ameaças cibernéticas. O trabalho também almeja pesquisar os métodos utilizados para o crescimento do (neo)terrorismo e as respectivas sanções implementadas na lei penal, com intuito de controle e de prevenção dos atos terroristas, bem como confrontar as ideias normativas do direito ao novo terrorismo as fontes da racionalidade penal orientada a combater a disseminação dos ataques terroristas e o seu crescimento.

O trabalho em questão também irá demonstrar a relevância de abranger o tema em pauta, visto que o novo terrorismo tem relação direta com a Legislação Penal e a Lei 13.260/2016, haja visto que ambas possuem dispositivos expressos que visam a prevenir ataques terroristas promovidos por grupos terroristas.

Ademais, os grupos terroristas tiveram considerável aumento a partir do século XXI, com aprimoramento da disseminação de ameaças cibernéticas, razão por que é necessário o estudo do tema mencionado, para fins para resultados positivos com relação à prevenção e repressão à expansão dos atos terroristas e dos principais grupos.

O estudo sobre o (neo)terrorismo continua atraindo diversos olhares, resultando em um crescimento ascendente, principalmente na área jurídica. Observado essa perspectiva, verifica-se que é possível haver uma fragilidade da racionalidade da lei penal, aspecto pelo qual resultou na execução desta pesquisa.

A pesquisa possui natureza teórica observado que se vale de ideologias, conceitos e ideias já existentes, buscando reconstruir as teorias vigentes. O tratamento dos dados se dá de forma qualitativa, visto que esse aborda em específico o tema mencionado, com uma percepção mais profunda. Com relação aos objetivos propostos, estes são de caráter explicativo, visando a esclarecer os fatos geradores da expansão do (neo)terrorismo e das formas de ameaças cibernéticas. Ademais, no tocante aos procedimentos técnicos são bibliográficos,

documentais, jurisprudenciais e estudo de determinados casos. O método de abordagem utilizado é o hipotético-dedutivo.

A obra em questão, em seu primeiro capítulo, analisa o surgimento do terrorismo mundial, a conceituação do terrorismo e do (neo)terrorismo e realiza as distinções necessárias para compreender o tema. O segundo capítulo aborda a definição de ameaças cibernéticas, o modus operandi do (neo)terrorismo e do terrorismo cibernético, além de discorrer quanto aos principais grupos terroristas da atualidade. Ao cabo, o terceiro e último capítulo consiste na análise da Lei 13.260/2016 e na observância da carência do Código Penal em relação ao crime (neo)terrorismo.

1 O TERRORISMO E O (NEO)TERRORISMO

1.1 CONCEITO DE TERRORISMO

O estudo sobre terrorismo é complexo e multifacetado, razão por que, como primeira tarefa, a pesquisa cuidará da abordagem conceitual. A primeira alusão, ao conceito de terrorismo, foi feita pelo filósofo irlandês Edmund Burke em *Letters on a Regicide Peace* (cartas sobre uma paz regicida), no ano de 1790.

Entretanto, sempre que se trata acerca do terrorismo, há grande impasse em conceituar tal tema. Diante disso, inicialmente, a pesquisa passa a utilizar o conceito de Cuello Calón, citado por Cabette e Nahur (2017):

“Terrorismo significa a criação, mediante execução repetida de delitos, de um estado de alarme ou de terror na coletividade, ou em certos grupos sociais, para impor ou favorecer a difusão de determinadas doutrinas sociais ou políticas. (CABETTE e NAHUR, 2017, p. 101).

Em plano internacional, a Organização das Nações Unidas (ONU), no dia 08 de outubro de ano de 2004, mediante Resolução 1566, conceituou o terrorismo como:

“[...] atos criminosos, inclusive contra civis, cometidos com a intenção de causar a morte ou lesões corporais graves ou de tomar reféns com o propósito de provocar um estado de terror na população em geral, em um grupo de pessoas ou em determinada pessoa, intimidar a uma população ou obrigar a um governo ou a uma organização internacional a realizar um ato, ou se abster de realizá-lo”. (ONU, 2004).

Outrossim, no plano nacional, importante mencionar a visão do Exército Brasileiro que conceituou o termo terrorismo, na MD35-G-01, como sendo:

“Forma de ação que consiste no emprego da violência física ou psicológica, de forma premeditada, por indivíduos ou grupos, apoiados ou não por Estados, com o intuito de coagir um governo, uma autoridade, um indivíduo, um grupo ou mesmo toda a população a adotar determinado comportamento. É motivado e organizado por razões políticas, ideológicas, econômicas, ambientais, religiosas ou psicossociais”. (MD35-G-01).

Conforme aludido por LIRA (2018), a definição de terrorismo decorre de diversos fatores:

As organizações são multifacetadas e sempre inovam em meios de execução dos atos violentos. Assim também há inúmeros grupos terroristas, em sua maioria, com ideias e propósitos distintos. Esses matizes que identificam cada grupo terrorista terminam por criar entraves semânticos para se definir o que é terrorismo, qual sua finalidade e quais seus meios de operação. (LIRA, 2018, p.32-33).

De acordo com a visão de Raposo, o terrorismo é definido como:

Atos criminosos pretendidos ou calculados para provocar um estado de terror no público em geral, num grupo de pessoas ou em indivíduos para fins políticos são injustificáveis em qualquer circunstância, independentemente das considerações de ordem política, filosófica, ideológica, racial, étnica, religiosa ou de qualquer outra natureza que possam ser invocadas para justificá-los. (RAPOSO, 2007).

Como salientado por Cabette e Nahur a tarefa de conceituar a expressão terrorismo não é corriqueira, tampouco restrita, vez que esse provém ocasionalmente do atual cenário vivenciado. Contudo, com o passar dos anos foi possível confirmar que o terrorismo faz uso da violência como meio para amedrontar os seus alvos, seja por razões políticas, religiosas, cívicas etc (CABETTE, NAHUR, 2017, p. 12).

A Lei 13.260/16, conhecida como a Lei Antiterrorismo do Brasil, conceitua o terrorismo em seu artigo 2º da seguinte forma:

Art. 2º O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública. (LEI Nº 13.260/2016, art. 2º).

Como visto, não existe um conceito exato de terrorismo, em razão de algumas divergências na elaboração da definição de tal concepção, no entanto identificar o sentido negativo do que não se coincide como prática de terrorismo. Ademais, buscar apenas um conceito para terrorismo se mostra uma tarefa ineficaz, vez que a conceituação difere com relação ao propósito que busca exercer.

Entretanto, em relação ao terrorismo cibernético, há na doutrina melhor definição conceitual.

O terrorismo cibernético ou Ciberterrorismo, é o terrorismo que se utiliza da internet e dos aparelhos eletrônicos como meios para a realização dos ataques terroristas.

Nesse sentido, Baptista (2016) descreve o Ciberterrorismo como:

[...] um ataque deliberado e motivado por questões ideológicas, políticas ou religiosos contra sistemas de informação ou infraestruturas de TI com a finalidade de interromper serviços essenciais como o fornecimento de água, energia, serviços de emergência e hospitalares, sistemas financeiros, controle de tráfego aéreo e semelhantes. Ataques ciberterroristas, para serem considerados como tal, devem inculcar o terror, como comumente entendido, isto é, ter como resultado mortes e/ou destruição em larga escala, e devem ter uma motivação política, ideológica ou religiosa. A simples utilização de computadores pelos terroristas como um facilitador de suas atividades, seja para propaganda, recrutamento, mineração de dados, comunicação ou outros fins, não é ciberterrorismo. (BAPTISTA, 2016).

Na mesma linha, Pinto (2011) conceitua Ciberterrorismo como:

Actos fundados em motivações políticas, ideológicas ou sociais e em operações de hacking com o objectivo de causar prejuízos severos (perda de vidas humanas, prejuízos econômicos, ataques ou ameaças contra sistemas informáticos, redes e a respectiva Informação neles armazenada) de forma a intimidar ou coagir um governo. Pode chegar a ser um ataque físico com o objectivo de destruir nos computadorizados de infraestruturas críticas (internet, telecomunicações) ou a grelha elétrica de um país ou de uma cidade. O Ciberterrorismo é semelhante ao cibercrime, mas é uma versão mais extrema do cibercrime, com consequências piores. Não existe uma definição normalizada (standard) de Ciberterrorismo e de ciberterrorista, que agrade a todos, pois a diferença entre hacking normal e Ciberterrorismo depende apenas da motivação do ataque (político ou pessoal). Ou seja, quando é pessoal ocorre apenas um ataque de hacking, mas se houver outras motivações poderá passar a ser considerado um acto ciberterrorista. Independentemente da motivação, ambos podem ser punidos pelo Computer Fraud and Abuse Act¹ dos EUA. Na Europa existe uma tentativa de harmonização entre as leis da União Europeia e dos EUA, o que significa que existem muitas semelhanças nas leis aprovadas e em vigor. (PINTO 2011, p.7)

O conceito da expressão Ciberterrorismo ou Terrorismo Cibernético, também é aduzida por Barreto para quem o tema:

Refere-se ao emprego, por terroristas, de técnicas de destruição ou incapacitação de redes computacionais de informação. Entre essas redes, destaca-se a internet, em razão do seu crescente fluxo de informações, importância, abrangência e extensão geográfica. Por isso, especialistas em Terrorismo Cibernético costumam apoiar-se na concepção de cenários possíveis, mediante avaliações feitas a partir da quantificação das (1) vulnerabilidades conhecidas e existentes nos sistemas informatizados, das (2) ameaças hipotéticas e reais que sobre

eles incidem, e, finalmente, do (3) valor estratégico, político ou econômico das informações operadas nesses sistemas. (BARRETO, 2017, p.63).

Assim, o terrorismo cibernético é usufruído pelos grupos terroristas, com o intuito de inviabilizar as redes de informação, bem como arruinar os aparelhos eletrônicos, principalmente os que estão ligados à internet, visando causar o maior número de prejuízos possíveis, com a máxima agilidade de disseminação das ameaças. A facilidade de acesso a rede mundial de computadores, tornou mais fácil e eficaz obter riquezas de modo ilícito, sem haver precisar que o criminoso saia de sua residência para praticar o crime (AGNOLETTO e BEZERRA, 2020, p. 52-53).

1.2 SURGIMENTO DO TERRORISMO E DO (NEO)TERRORISMO

O terrorismo surge no século I d. C, enfatizando-se cada vez mais com o passar dos anos. O termo terror era tido como um conceito político, surgindo como um regime utilizado por grupos isolados para enfrentar o Estado de forma direta, tendo como principal método a violência, introduzido pelos jacobinos de Robespierre, durante o ano de 1793, junto com a Revolução Francesa (FRAGOSO, 1981, p. 14).

Conforme aludido por WOLOSZYN, o terrorismo sempre esteve presente na história da humanidade:

Estima-se que tenha surgido durante a república romana no séc. III a.C. como tática militar sob o nome de guerra destrutiva ou guerra punitiva, utilizada pelos exércitos conquistadores para afetar o comportamento de populações e líderes das nações dominadas, através do cometimento de ações atroztes contra a população civil, com o objetivo de causar terror e pânico, impedindo desta forma, o apoio desta população a líderes locais, por temor a represálias. (WOLOSZYN, 2005).

O terrorismo tem como objetivo mostrar ao mundo e principalmente aos seus inimigos o propósito de sua luta, mesmo que, para alcançarem seus fins, coloquem em risco a vida de diversas pessoas, dando para a causa, a sua própria vida, quando necessário. Utiliza-se o termo luta, visto que os membros dos grupos terroristas avistam seus atos como uma forma de luta, um meio de combate e não como um crime (PETERKE, 2014).

De acordo com Hudson, tem-se como a uma das primeiras referências expressas sobre o terrorismo o Sicarii (homens punhais), que se infiltravam nas cidades comandadas pelos romanos, empregando o terror como meio estimular a modificação na sociedade judaica da época (HUDSON, 1999, p.12).

Outrossim, merece nota que o terrorismo e a guerra não se confundem, pois, de acordo com CALLEGARI, LIRA, REGHELIN, MELIÁ e LINHARES, o método utilizado pelo Estado para combater o terrorismo, possuindo relação direta na diferenciação entre ato terrorista e ato de guerra. O fato é que cada termo possui particularidades distintas, bem como resultados divergentes, não sendo possível empregar a mesma conduta para ambos (CALLEGARI; LIRA; REGHELIN; MELIÁ; e LINHARES, 2016, p.67).

Já o (neo)terrorismo, surge em meados do século XIX, após a revolução francesa, já que “A história do mundo desde a Primeira Guerra Mundial tomou forma à sombra de Lenin, real ou imaginário, como a história do mundo ocidental no século XIX tomou forma à sombra da Revolução Francesa.” (HOBSBAWN,1914, p. 288). Todavia, esse teve como obstáculo principal os ataques terroristas de 11 de setembro de 2001, sucedendo na queda das torres gêmeas e na morte de inúmeros civis, ato o qual foi ordenado pelo grupo islâmico da al-Qaeda, direcionados aos Estados Unidos.

De acordo com Teixeira da Silva, o (neo)terrorismo ocorre com a reestruturação dos movimentos mujjahidin (os chamados afegãos), a partir do ano de 1993, possuindo como marco principal o atentado contra World Trade Center, planejado por uma das organizações terceirizadas pela Al Qaeda (TEIXEIRA DA SILVA, 2001, p. 44-45).

O (neo) terrorismo expõe algumas particularidades, as quais o diferem do terrorismo antigo, segundo WITCKER:

“[...] o caráter transnacional; o embasamento religioso e nacionalista; o uso de terroristas suicidas; a alta letalidade dos ataques; e a orientação anticidental, sobretudo nos grupos fundamentalistas islâmicos. Essas características nos remetem a uma nova modalidade, que poderia ser chamada de neoterrorismo [...]”. (WITCKER, 2005).

Conforme aludido por Veiga, o (neo)terrorismo é dividido em ciclos, sendo o ciclo anarquista, o ciclo anticolonial, o ciclo esquerdista e o ciclo religioso. No início do ano de 1880 surge o ciclo anarquista, de origem Russa, sendo o

responsável pela mobilização do terrorismo global, movido pela carência das alterações defendidas por Czar Alexandre II (VEIGA, 2018, p.16).

Veiga aduz que ciclo anticolonial tem início em 1920, decorrente do tratado de paz de Versailles, o qual visava abater os impérios dominados com o fim da Primeira Guerra Mundial. Já o ciclo esquerdista teve origem no ano de 1960, motivado pela Guerra do Vietnam, no qual trouxe à tona novamente algumas particularidades do primeiro ciclo, sendo conhecida pelos sequestros de aeronaves e reféns. Tem-se o ciclo religioso como quarto ciclo, começando no ano de 1979 e possuindo o islamismo como ponto central, despertado pelo início de novo século no calendário muçulmano, a Revolução Iraniana e a invasão do Afeganistão pela União Soviética (VEIGA, 2018, p.17-19).

A distinção do antigo terrorismo e do (neo)terrorismo, pode ser verificada em diversas características como, o espaço utilizado na prática dos atos terroristas, as vítimas, o armamento, os locais dos atentados e os recursos financeiros.

1.3 DISTINÇÕES NECESSÁRIAS

É possível verificar que para muitos indivíduos o terrorismo e a guerra são considerados como uma só ação, pressupondo que ambos os conceitos seriam sinônimos de um para o outro. Contudo, ambos são fenômenos distintos conforme aludido por Wilkinson, o autor destaca o impasse na diferenciação clara do ato de terrorismo e do ato de guerra (WILKINSON, 1976, p.19).

No mesmo sentido Meliá aduz que o terrorismo necessita de controle militar, exatamente por não se configurar como ato de guerra, sendo que esse caracteriza uma tática de um grupo mais tênue, carecendo de uma similar à força militar da qual não dispõe. Já o ato de guerra é realizado perante um enorme combate armado (MELIÁ, 2010, p. 70).

Segundo, Callegari; Lira; Reghelin; Meliá e Linhares:

A diferenciação entre ato terrorista e ato de guerra importará em consequências diretas na forma de combate ao terrorismo a ser adotada pelo Estado. Isso se deve ao fato de ambos os fenômenos exigirem formas diferentes de abordagem, levando-se em conta suas motivações e consequências especiais. (CALLEGARI; LIRA; REGHELIN; MELIÁ; LINHARES, 2017, p.67).

Por mais que ambos os atos se pareçam de maneira muito similar, podemos observar que os principais pontos que os distinguem são as suas finalidades, bem como a escassez ou o excesso de armamentos (poder de fogo) utilizados por um ou pelo outro.

Veja-se, por exemplo, que também não se pode confundir a conduta de genocídio com o terrorismo.

O Genocídio possui como finalidade a exterminação de determinado grupo étnico, religioso ou racial, conforme tipificado no artigo 1º da Lei nº 2.899/56:

Art. 1º Quem, com a intenção de destruir, no todo ou em parte, grupo nacional, étnico, racial ou religioso, como tal:

- a)** matar membros do grupo;
- b)** causar lesão grave à integridade física ou mental de membros do grupo;
- c)** submeter intencionalmente o grupo a condições de existência capazes de ocasionar-lhe a destruição física total ou parcial;
- d)** adotar medidas destinadas a impedir os nascimentos no seio do grupo;
- e)** efetuar a transferência forçada de crianças do grupo para outro grupo;

Será punido:

Com as penas do art. 121, § 2º, do Código Penal, no caso da letra a;

Com as penas do art. 129, § 2º, no caso da letra b;

Com as penas do art. 270, no caso da letra c;

Com as penas do art. 125, no caso da letra d;

Com as penas do art. 148, no caso da letra e;

No mesmo sentido, Lima aduz que por mais que os dois crimes sejam relativos com temas ligados à religião, à raça, à etnia e à nacionalidade, ambos não se misturam, principalmente por dois pontos:

- a) bem jurídico tutelado, sendo que para o terrorismo esse seria a paz pública, já para o genocídio seria a existência de um grupo específico (nacional, étnico, racial ou religioso). b) Especial fim de agir, que para o terrorismo é o de provocar o terror social ou generalizado, no entanto para o genocídio, é a intenção de destruir, no todo ou em parte, determinado grupo. (LIMA, 2020, p. 952).

Dessa forma, há relevante distinção pois o genocídio tem por finalidade o confronto direto com um grupo específico, visando sua destruição de forma total ou parcial, enquanto o Terrorismo tem como uma de suas principais características a generalização, levantando o terror social como um todo.

Da mesma forma, não se pode confundir ações terroristas com os atos praticados por movimentos sociais, ponto, inclusive, que foi objeto de muita divergência por ocasião da criminalização do terrorismo na legislação do Brasil.

Daí porque se defende que as manifestações sociais não podem ser confundidas com o terrorismo, conforme aludido por Cruz e Peixoto os manifestações sociais são utilizadas como forma de confrontar diretamente o Estado, são atos coletivos que possuem a influência da ideologia, bem como a pluralidade de personalidades (CRUZ, PEIXOTO, 2019, p.24-25).

No mesmo sentido Callegari, Lira, Reghelin, Meliá e Linhares aduzem que:

As manifestações sociais não objetivam disseminar o sentimento de terror ou medo na população civil. Ao contrário, em regra, desejam a população local ao seu lado, pois são identificados com eles e, muitas vezes, reivindicam em prol do grande grupo. (CALLEGARI, LIRA, REGHELIN, MELIÁ, LINHARES, 2016, p. 73).

Aliás, as manifestações sociais pós-moderno elevam a parcialidade do indivíduo, nesse bojo Braz aduz:

Apostou-se numa prática política que valorizasse o cotidiano, o dia a dia, o “aqui e agora”. As lutas sociais microscópicas são valorizadas através das experiências diversas vivenciadas pelos variados grupos sociais que se constituíam sujeitos coletivos. Aflora, com isso, a importância da dimensão subjetiva dos sujeitos, reivindicando o entendimento da subjetividade como reconhecimento da autonomia dos interesses variados presentes na sociedade civil e de seus respectivos grupos sociais. (BRAZ, 2012, p. 117).

Braz também se refere ao surgimento de uma política destinada a rotina, ao dia a dia, evidenciando-se uma sociedade subjetiva, assumindo de certa maneira uma fantasia real (BRAZ, 2012, p. 117).

Pode-se observar que as manifestações sociais envolvem a coletividade, tendo como alvo principal o Estado, não valendo-se da utilização do discurso de terror, muito menos da operacionalização do indivíduo. Ademais, não é possível embaralhar o terrorismo com as manifestações sociais, pois não há considerável ofensa ao bem jurídico tutelado.

Como visto, embora o terrorismo seja um tema complexo e multifacetado, dificultando sua compreensão, especialmente em relação a uma definição

jurídica, há, por exclusão, um conceito possível de ser formado, inclusive ao se diferenciar as ações terroristas de práticas semelhantes, mas, na essência, muito distintas.

Feita essa observação, no próximo capítulo a pesquisa cuidará da abordagem da expansão do terrorismo e de suas novas formas, além da forma de operação de seus agentes.

2 A EXPANSÃO DO (NEO)TERRORISMO E SEU “MODUS OPERANDI”

As formas de expansões do terrorismo são diversas. Porém, no caso da pesquisa, será estudado o ato terrorista cometido a partir da expansão dos meios de comunicação, notadamente a rede mundial de tráfego de dados. Não há como conceituar de forma direta e simples o que seriam as ameaças cibernéticas, no entanto, de acordo com o Manual MD35-G-01, essas podem ser consideradas como:

Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de comunicações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil. (MD35-G-01, p2007).

O Manual Doutrina de Defesa Cibernética – MD31-M-07 (BRASIL, 2017, p. 18) também conceituou ameaça cibernética como sendo “[...]causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse”.

As ameaças cibernéticas estão ligadas diretamente ao cibercrime, tornando-se um modo extremamente eficaz e ágil para a realização de ataques pela internet, utilizando a rede de computadores e os demais sistemas de informações como um meio poderoso.

Conforme relatado pelo 11º Congresso das Nações Unidas sobre Prevenção do Crime e Justiça Penal realizado na Tailândia, no ano de 2005:

Os crimes informáticos são difíceis de captar e de conceptualizar. Frequentemente, considera-se que constituem uma conduta proscribida pelas legislações e/ou jurisprudência, que implica o uso de tecnologias digitais para cometer o delito; que é dirigida contra as próprias tecnologias da informação e comunicação; ou que envolve o uso de acessório de equipamento informático na prática de outros crimes. (TAILÂNDIA, 2005).

É nítido que, com o passar dos anos a internet e os aparelhos eletrônicos evoluíram de forma surpreendente, ocasionando um “upgrade” e impulsionando as inovações para a implementação de novas ameaças cibernéticas.

São diversos os tipos de ameaças cibernéticas existentes, todavia pode-se referenciar as 06 (seis) formas mais comuns e utilizadas, de acordo com Baptista:

Phishing: É o ato de tentar enganar os clientes a fornecer suas informações de segurança pessoal; seus números de cartão de crédito, detalhes de contas bancárias ou outras informações confidenciais, fazendo-se passar por empresas confiáveis em um e-mail. As mensagens podem pedir aos destinatários a “atualizar”, “validar” ou “confirmar” as informações da conta.

Spam: Outra forma de cibercrime é o spam. Sem dúvida é o produto da mais profunda capacidade da Internet de colocar poderes sem precedentes nas mãos de uma única pessoa. O e-mail de spam é a distribuição de e-mails em massa que anunciam produtos, serviços ou esquemas de investimento, que podem muito bem ser fraudulentos. O objetivo do spam é enganar os clientes e levá-los a acreditar que irão receber um produto ou serviço genuínos, geralmente a um preço reduzido.

Hacking: é uma das formas de cibercrime mais amplamente analisada e debatida. Representa um intenso foco de preocupações do público sobre a ameaça que essa atividade representa para a sociedade. Os ataques ocorrem em diversas fases, como a coleta de informações ou de reconhecimento, verificação e, finalmente, entrar no sistema de destino. A coleta de informações envolve métodos de obtenção de informação ou abrir brechas de segurança. É assim como a maneira em que o tipo tradicional de furto é realizado.

Assédio cibernético ou bullying: Ciberassédio ou bullying é o uso de dispositivos de informação e comunicação eletrônicos, como e-mail, mensagens instantâneas, mensagens de texto, blogs, telefones celulares, pagers, mensagens instantâneas e páginas web com conteúdo difamatório para intimidar ou assediar um indivíduo ou grupo por meio de ataques pessoais ou outros meios.

Furto de identidade: Este é o tipo de fraude que apresenta o mais rápido crescimento no Reino Unido. O furto de identidade é o ato de obter informações confidenciais sobre outra pessoa sem o seu conhecimento, usando esta informação para cometer outros crimes.

Fraude de cartão de plástico: Fraude de cartões de plástico é o uso não autorizado de cartões de plástico ou de crédito ou o roubo de cartões para saque de dinheiro ou obtenção de bens. (BAPTISTA, 2016).

Como se vê, deve-se ressaltar que as ameaças cibernéticas são realizadas dentro do espaço cibernético, o qual também é conceituado pelo Manual Doutrina de Defesa Cibernética – MD31-M-07 (BRASIL, 2017, p. 18) como “[...]espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas”.

O mesmo Manual também definiu o conceito de cibernética, como sendo:

Termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de

computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais. (MD31-M-07, 2017, p. 18).

Barbosa e Alves mencionam as diferenças do cibercrime para o ciberterrorismo, sendo que:

Chama-se de cibercrime atos que envolvam qualquer prática ilícita dentro da rede digital ou que se utilizam dos instrumentos eletrônicos para a colaboração do crime. Algumas dessas práticas criminosas são roubo de dados pessoais, disseminação de vírus em redes, usurpação de sistemas, invasão a elementos sigilosos, entre outros. Por outro lado, se tem o ciberterrorismo, uma ramificação mais perigosa e avançada do cibercrime, com o objetivo de cometer ataques contra um grupo maior de pessoas ou até mesmo contra o próprio Estado. (BARBOSA e ALVES, 2021).

De acordo com Agnoletto e Bezerra:

Para o combate ao cibercrime transnacional é fundamental a coleta, armazenamento, lapidação e análise das diversas condutas criminosas perpetradas, visto que vários são os crimes cometidos de forma conexa e acompanhada, restando nesta ferramenta a maneira mais eficiente de se buscar os elos de ligação para a captura de criminosos e quadrilhas especializadas no cibercrimes, onde quer que eles se encontrem, no território pátrio ou estrangeiro. (AGNOLETTO e BEZERRA, 2020, p. 20).

Por tudo que se lê até aqui, pode-se concluir, ainda que de forma não definitiva, que as ameaças cibernéticas são ataques realizados com o emprego de meio disponíveis no espaço cibernético, utilizando os aparelhos eletrônicos e a internet como alguns dos meios mais rápidos para produzir danos aos inimigos, danos esses que por muitas vezes são irreparáveis.

A seguir, a pesquisa abordará melhor o emprego desses meios nos atos terroristas, a fim de traçar uma melhor compreensão do ‘modus operandi’.

2.2 *MODUS OPERANDI* DO (NEO)TERRORISMO E TERRORISMO CIBERNÉTICO E SUAS FINALIDADES

O (neo)terrorismo, como o próprio nome sugere, é uma das novas formas de terrorismo, distinguindo-se do terrorismo clássico em diversos pontos como,

as formas de ataques, seus alvos, suas motivações entre outras particularidades.

De acordo com Veiga (2018), o terrorismo é categorizado por algumas fases, as quais são denominadas como “ondas”. O autor refere que tais ondas podem ser encaradas como transitórias e sistemáticas, uma vez que apresentam *modus operandi* distintos e que possuem um período de duração, se estendendo por aproximadamente uma geração (VEIGA, 2018, p. 16).

Para Leite (2020), o surgimento da quinta onda poderá transcorrer com a chegada de novos meios de ataques, que têm característica de menos onerosos e com grandes impactos, como o ciberterrorismo, tendo em vista a consolidação dos grupos radicais e a busca por recursos mais eficientes (LEITE, 2020, p. 22).

Nesse mesmo sentido, Leite (2020) aduz sobre o *modus operandi* do (neo)terrorismo, de maneira que:

O terrorismo atual apresenta ataques com alto grau de letalidade, sem nenhum comprometimento dos terroristas com a ética e a moral. Tem como característica selecionar alvos aleatórios, o emprego da violência indiscriminada em larga escala, bem como a mudança dentro da organização terrorista, para a estrutura de células descentralizadas e independentes e que não interagem horizontalmente. Essas estruturas dificultam sobremaneira a identificação e eliminação de ações dessa natureza, exigindo o aperfeiçoamento das técnicas de Guerra ao Terror. (LEITE, 2020, p. 22).

O (neo)terrorismo busca utilizar métodos mais eficientes e menos custosos para a realização dos ataques terroristas, de modo que alcancem suas finalidades de maneira mais célere. Ademais, estão sempre buscando mecanismos de inovação para a realização de seus ataques, bem como táticas para o recrutamento de novos seguidores.

Conforme salientado por Coelho (2019) o novo terrorismo, principalmente pós ataques de 11 de setembro, intensificou a utilização das tecnologias, em especial as formas de transmissão como à internet, a fim de facilitar a prática de seus atos terroristas (COELHO, 2019, p. 57/58).

Atualmente, o terrorismo cibernético ou ciberterrorismo é tido como um dos principais e favoritos *modus operandi* para a realização dos ataques ordenados por grupos terroristas, porquanto possuem um grande nível de alastramento.

Na mesma linha, Coelho (2019) expõem sobre o fortalecimento no uso da internet:

O crescimento da utilização da internet na execução de atentados foi provavelmente proporcionado pela combinação entre novas tecnologias e o maior foco das forças de segurança na movimentação de potenciais terroristas, sobretudo os que retornam de zonas de conflito como a Síria e Iraque. Verificou-se ainda que a ampliação dessa nova forma de utilização da internet coincidiu com o aumento do terrorismo de “ator único” na Europa. (COELHO, 2019, p. 61).

Segundo Weimann, *apud* Chagas (2012), o ciberterrorismo está se tornando um dos métodos mais utilizados pelos grupos terroristas, tendo em vista seu baixo custo, seu anonimato em relação aos demais meios e a sua grande variedade e número de alvos disponíveis, possibilitando ataques às empresas públicas e privadas, aos governos mundiais e aos próprios cidadãos de todo o mundo (WEIMANN, *apud* CHAGAS, 2012, p. 34).

Não há como identificar apenas uma finalidade com relação ao (neo)terrorismo, uma vez que os ataques terroristas se valem de inúmeras motivações como a política, a religião, preconceito de raça, etnia, entre diversas outras.

Para Diniz, a finalidade do (neo)terrorismo seria o emprego da violência em pessoas, as quais geralmente fazem parte de um grupo específico, com o intuito propagar medo e fazer a divulgação de seus atos terroristas, bem como o porque da realização de tais atos (DINIZ, 2002, p. 5).

Diniz, então, conclui que o (neo)terrorismo possui como finalidade/alvo principal as questões políticas:

[...] o terrorismo é uma etapa de uma seqüência de ações que visa a produzir um fim político desejado, sendo melhor caracterizado, portanto, como parte de uma estratégia, algo que definimos como um estratagema; difere de outras formas de emprego da força pela maneira específica como a emprega (o terror) e de outras formas de emprego do terror por não visar nem a compelir nem a dissuadir, mas sim a induzir no inimigo um comportamento que altere a relação de forças em favor do grupo terrorista. (DINIZ, 2002, p. 15).

Entretanto, os atos terroristas, na atualidade, não estão ligados preponderantemente à política, uma vez que com o passar dos anos surgiram

outras causas passíveis de motivar grupos terroristas na realização de novos ataques.

Já para Hoffman, citado por Alcântara, o (neo)terrorismo é planejado para impor poder em determinados lugares, nos quais ainda não exista poder ou em locais que o tamanho do poder ainda não seja abundante. Ademais, refere esse autor que os atos terroristas visam causar terror psicológico a longo prazo nas vítimas (HOFFMAN, citado por ALCÂNTARA, 2018, p. 56).

O ciberterrorismo, por sua vez, possui suas finalidades de uma maneira mais clara e objetiva, conforme referido por Alcântara:

[...] o ciberterrorismo aparece com o uso ativo do ciberespaço, com operações focadas na mobilização de pessoas (alvo das ações é a mente humana) e na invasão e destruição de sistemas e dados tecnológicos, principalmente de Infraestruturas Críticas (IC). Em outras palavras, há um viés estratégico no uso do ciberespaço, objetivando o enfraquecimento do oponente, e não apenas o uso do ciberespaço como um multiplicador de força. (ALCÂNTARA, 2018, p. 83-84).

Baptista também refere sobre a finalidade do ciberterrorismo, de modo que:

[...] a finalidade de interromper serviços essenciais como o fornecimento de água, energia, serviços de emergência e hospitalares, sistemas financeiros, controle de tráfego aéreo e semelhantes. Ataques ciberterroristas, para serem considerados como tal, devem incutir o terror, como comumente entendido, isto é, ter como resultado mortes e/ou destruição em larga escala, e devem ter uma motivação política, ideológica ou religiosa. A simples utilização de computadores pelos terroristas como um facilitador de suas atividades, seja para propaganda, recrutamento, mineração de dados, comunicação ou outros fins, não é ciberterrorismo. (BAPTISTA, 2016).

Para Lehfeld, Nunes e Silva, a sociedade moderna evoluiu consideravelmente com relação as tecnologias, sendo esse um dos principais motivos dos danos realizados por ciberterroristas à segurança do Estado (LEHFELD; NUNES e SILVA, 2020, p. 3).

Os mesmos autores aduzem que os ataques advindos do ciberterrorismo, são realizados diretamente contra o Estado, de modo que podem gerar uma intervenção na atuação de soberania, conforme aludido a seguir:

Essa espécie de cibercriminalidade visa difundir o terrorismo comum no ciberespaço, abrangendo todo o âmbito transnacional para,

eficazmente, disseminar o terror e que podem acarretar diretamente em uma interferência no poder soberano, pois o ato é praticado contra o Estado. Isto ocorre justamente pela crise que a soberania sofre quando confrontada com a globalização, pois o último é o meio em que o ciberterrorismo se impõem. (LEHFELD; NUNES e SILVA, 2020, p. 3).

Nesse sentido, menciona Tangerino:

Como destacam os especialistas em ciberespaço, com o aumento da conectividade global e a ampliação dos grupos extremistas, os instrumentos tradicionais de controle e prevenção criminais se tornarão inócuos – se já não o são atualmente – sendo certo que se demonstrarão cada vez mais ineficazes no combate ao crime, em especial aos atos de terror cibernéticos. (TANGERINO, 2016).

Agnoletto e Bezerra conceituam os crimes cibernéticos mistos, como sendo:

Crimes cibernéticos mistos são aqueles em que não apenas se utiliza a tecnologia para a comissão delitiva, mas onde esta se torna imprescindível ou ao menos toma o delito particularmente ofensivo ou lesivo. Crimes como os de pornografia infantil pela internet e as fraudes bancárias eletrônicas exemplificam essa classificação. (AGNOLETTO e Bezerra, 2020, p. 52).

Sendo assim, constata-se que o (neo)terrorismo utiliza como *modus operandi* a realização de ataques com um imenso nível de mortandade, marcados pelo emprego de violência física e psicológica em seus alvos, sem haver o acatamento das regras da moral e da ética pelos membros dos grupos, tendo como finalidade disseminar o medo, a fim de dominar determinados grupos ou até mesmo indivíduos, com base em suas motivações.

No tocante ao “modus operandi” do ciberterrorismo, esse emprega o uso de novas tecnologias para a realização de ataques na internet, valendo-se dos diversos tipos de ameaças cibernéticas para alcançar o seu objetivo de maneira eficiente, de modo que sua finalidade visa a destruir ou danificar consideravelmente sistemas de informações, também contando com a aplicação da violência.

O próximo item analisará os principais grupos que promovem ações violentas terroristas.

2.3 OS PRINCIPAIS GRUPOS TERRORISTAS DA ATUALIDADE

Com o surgimento do (neo)terrorismo houve manifestação de novos grupos terroristas, no entanto há grupos específicos, os quais são responsáveis pela maioria dos ataques terroristas, tornando-se esses os principais grupos terroristas da atualidade.

De acordo com Dudley, existem 5 (cinco) grupos terroristas mais atuantes, a saber o (Estado Islâmico, o Taleban, o Al-Shabaab, A Al-Qaeda e Boko Haram) que são responsáveis pela maioria das ações que resultaram na morte de mais de 18.000 mil pessoas até o ano de 2018. Ademais, no ano de 2017, esses grupos foram os culpados pela morte de 10.632 mortes, sendo que nos últimos 10 anos, os mesmos grupos tornaram-se responsáveis por 44% dos óbitos decorrentes do terrorismo. (DUDLEY, 2018). Já no ano de 2021, os grupos terroristas causadores pela maioria das mortes foram o Estado Islâmico, Al shabaab, Talibã e Jamat Nusrat Al-Islam wal Muslimeen (JNIM), sendo que no ano de 2020 três desses grupos estavam elencados como os mais letais (INSTITUTE FOR ECONOMICS & PEACE, 2018).

O Estado Islâmico, também conhecido por (ISIL) e (ISIS), do ano de 2016 até o ano de 2018, era tido como o grupo terrorista mais fatal, uma vez que além das atividades de sequestro e assassinato, o grupo também deliberava bombardeios e explosões (INSTITUTE FOR ECONOMICS & PEACE, 2018).

O ISIL opera, especialmente no Iraque e na Síria e, também estava ativo, até 2017, em dez países, sendo que realizou 286 ataques em quatro regiões diferentes na época. Contudo, após 2017, o grupo teve uma diminuição significativa no Iraque e na Síria, o que resultou na perda de 20% de sua receita e 60% de seu território, decaindo seu rendimento na criação de um califado (INSTITUTE FOR ECONOMICS & PEACE, 2018).

Também houve uma diminuição de 68% no número de mortes advindas dos ataques da ISIL na Europa, reduzindo de 198 mortes em 2016 para 64 mortes em 2017. Além disso, com base em todos os ataques realizados pelo ISIL, verifica-se que 98% das mortes e dos incidentes aconteceram na Região do Oriente Médio e no Norte da África (INSTITUTE FOR ECONOMICS & PEACE, 2018).

Por sua vez, o Al-Shabaab é caracterizado por ser um grupo militante extremista, o qual teve origem em 2006, após a realização de uma competição, a qual visava o controle da capital da Somália, operando em diversos países como a Quênia, Etiópia e Uganda, no entanto o principal país de atuação deste grupo terrorista é a Somália. O Al-Shabaab está associado diretamente a Al-Qaeda, buscando também, a construção de um estado islâmico em seu país de origem (DUDLEY, 2018).

Esse grupo terrorista, em 2017, foi considerado como o mais letal na África subsaariana, tendo em vista o aumento de 93% de mortes advindas de ataques ministrados pelo Al-Shabaab, os quais ocasionaram mais de mil mortes no mesmo ano. Também no ano de 2017, o grupo foi responsável por uma explosão que ocorreu fora do hotel Safari, localizado na capital Mogadíscio, resultando no óbito de 588 pessoas e 316 feridos (INSTITUTE FOR ECONOMICS & PEACE, 2018).

O Al-Shabaab faz uso de diversas táticas que resultaram no sucesso de seus ataques, motivo pelo qual sobejou o Boko Haram em 2017, o qual sustentava o título de grupo terrorista mais mortal até aquele momento. No mesmo ano, o grupo realizou ataques que possuíam como objetivo diretamente o governo de seu país e seus respectivos agentes (INSTITUTE FOR ECONOMICS & PEACE, 2018).

Já o Talibã teve origem no Afeganistão em 1994, conhecido por ser um grupo revolucionário, o qual em 1996 assumiu o controle de seu país de origem, anunciando o mesmo como um califado islâmico. Em 2001, a OTAN realizou uma invasão no Afeganistão, apartando o Talibã do país, no entanto com o passar dos anos o grupo está reavendo, de maneira gradativa o controle de seu território de origem (INSTITUTE FOR ECONOMICS & PEACE, 2018).

Durante o ano de 2017, o Talibã administrava aproximadamente 11% de seu país, além de na época estar litigando em torno de 29% dos 398 distritos localizados no Afeganistão. Os ataques realizados pelo grupo no decorrer de 2017, resultaram na morte de inúmeros policiais e militares, uma vez que o grupo foi o causante praticamente 700 ataques, sucedendo o óbito de 3.571 pessoas (DUDLEY, 2018).

Outrossim, o Talibã opera em 70% das províncias do Afeganistão, motivo pelo qual se tornou muito vigiado pelas autoridades, principalmente pelos

militares, posto que 54% de seus ataques são realizados mediante atentados a bomba e assaltos armados, sendo esses os preferidos do grupo terrorista (DUDLEY, 2018).

Outro grupo relevante no cenário é Al-Qaeda, surgida por volta da década de 70 e 80, com o intuito de ajudar a impedir a invasão por parte da união soviética, em decorrência da Guerra Fria, além disso o grupo recebia auxílio dos EUA, o qual fornecia além do treinamento, equipamentos, armas e munições para o grupo. Um dos grupos terroristas mais conhecidos do mundo, responsável pelos famosos ataques realizados em 11 de setembro de 2001 na cidade de Nova York, sendo estes ordenados pelo líder do grupo, Osama Bin Laden, tornando-se o principal antagonista dos Estados Unidos.

Após os ataques de 11 de setembro, a Al-Qaeda recebeu muitos olhares do mundo inteiro, provocando o entusiasmo de inúmeros grupos terroristas e obtendo novos admiradores. Tais ataques podem ser considerados como um dos marcos do (neo)terrorismo (INSTITUTE FOR ECONOMICS & PEACE, 2018).

De acordo com Lawrence, mesmo após os ataques de 11 de setembro a Al-Qaeda ainda mantinha células terroristas adormecidas nos EUA:

(...)concluiu que a Al-Qaeda possuía células dormentes ocultas nos Estados Unidos. Os vínculos entre as células canadenses e jordanianas apontavam para o seu país. Porém, mesmo após os ataques às embaixadas americanas e a tentativa de lançar uma bomba no aeroporto de Los Angeles, a direção do fbi continuava vendo a Al-Qaeda como uma ameaça distante e controlável. (LAWRENCE, 2006, p. 242).

O grupo teve uma grande ascendência durante o século XXI, tornando-se um dos principais grupos terroristas do (neo)terrorismo. A Al-Qaeda vem desenvolvendo seus métodos de ataques e objetivando de forma mais inteligente os seus alvos, buscando resultados imediatos e com grande impacto, gerando um alto nível de letalidade. Além disto, veio conquistando e recrutando inúmeros seguidores, os quais se identificaram com as causas que motivam o grupo terrorista.

Por último, mas não menos importante, há o grupo Boko Haram, tendo como significado “a educação ocidental é um pecado”, é caracterizado pela violência extrema e por sua crueldade. Também conhecido como Jama’tu Ahlis

Sunna Lidda'awati wal-Jihad, é tido como a organização mais trágica da África Subsaariana até 2017. Boko Haram é considerado como o grupo terrorista mais mortífero do mundo, sendo esse o grupo vivo na Nigéria, mesmo com sua decaída em 2014 (INSTITUTE FOR ECONOMICS & PEACE, 2018).

Esse grupo terrorista teve origem no Nordeste da Nigéria, fundado por Mohammed Yusuf em 2002. Entretanto, desde 2009 o grupo é liderado por Abubakar Shekau, vindo a aprimorar-se em explosões e bombardeios de elevada repercussão. Além disso, o grupo terrorista Boko Haram faz uso das táticas terroristas mais excêntricas como a utilização de mulheres e crianças como suicidas, além do uso amplo de crianças, sendo que em 2016, de cinco atentados, quatro foram realizados por indivíduos do sexo feminino (INSTITUTE FOR ECONOMICS & PEACE, 2018).

De acordo com os dados, em 2017 o grupo terrorista Boko Haram realizou dez ataques terroristas mais mortais, sendo que todos esses ataques foram realizados dentro da Nigéria, a maioria no estado de Borno, motivo pelo qual 81% dos óbitos decorrentes dos ataques, deram-se na Nigéria (INSTITUTE FOR ECONOMICS & PEACE, 2018).

No Brasil, um marco histórico do (neo)terrorismo foi a Operação Hashtag, realizada pelo DAT (Departamento Antiterrorismo da Polícia Federal), em julho de 2016. Nesta operação, houve a desmobilização de jovens radicalizados, sendo utilizada pela 1ª vez a Lei nº 13.260/16 – Lei Antiterror, conforme denúncia realizada pelo MPF (Ministério Público Federal), na qual consta que:

De 17 de março a 21 de julho de 2016, os denunciados, de forma livre e consciente da ilicitude de suas condutas, promoveram a organização terrorista Estado Islâmico do Iraque e do Levante (EIIL) ou Estado Islâmico do Iraque e da Síria¹, por meio de publicações em redes sociais, troca de materiais e diálogos em grupos de aplicativos. Em inúmeras ocasiões, os denunciados demonstraram devoção à organização terrorista, afirmando, inclusive, intenção de ação terrorista no decorrer dos Jogos Olímpicos Rio 2016 e objetivo de reunião física para preparação e treinamento para futura migração à região de dominação do grupo extremista. (MPF, denúncia, 2016, p. 3).

A realização da Operação Hashtag, se deu após o conhecimento de publicações e diálogos de alguns indivíduos, as quais demonstraram cunho radical, constatando-se apoio integral e incentivo às ações do grupo extremista EI. Ademais, verificou-se a existência de vídeos e imagens que possuíam caráter

de veneração à ideologia do grupo terrorista, conforme expresso pela denúncia do Ministério Público Federal (MPF).

A investigação foi realizada pelo DAT (Divisão Antiterrorismo da Polícia Federal), na qual SE constatou a ligação direta de 14 (quatorze) brasileiros com outros participantes do grupo terrorista Estado Islâmico. Além disso, verificou-se a possível realização de um ataque terrorista nos jogos olímpicos de 2016, com base em trocas de mensagens realizadas por redes sociais como o Facebook, Twitter, Instagram e Telegram, pelos integrantes do grupo terrorista, os quais se autointitulavam como “Defensores da Sharia”.

Diante de tais fatos, o MPF denunciou 8 (oito) dos 14 (quatorze) suspeitos de integrarem o grupo terrorista, referindo que:

[...] os denunciados, em diálogos, trocaram informações acerca do Estado Islâmico, inclusive sobre os meios de migração para integração física da organização extremista e sobre como realizar o juramento (bay'at) ao líder da organização (Abu Bakr al-Baghdadi²) pela internet. Ainda, comemoraram ataques reivindicados pelo Estado Islâmico, a exemplo dos ataques na França (Paris e Nice) e Orlando/EUA e reverenciaram os seus responsáveis (como Omar Mateen, autor dos ataques em Orlando/EUA). Em mais de uma ocasião, os denunciados abordaram, em diálogos, a oportunidade de atuação terrorista no decorrer da Olimpíada (Rio 2016), diante do momento excepcional, de protagonismo do Brasil no cenário internacional. Apontaram, também, a presença de indivíduos de diversas nacionalidades no País, o que expandiria a repercussão dos atos em planejamento. Demonstraram inequívoca vontade de atuação neste evento internacional, ante ao seu simbolismo. (MPF, denúncia, 2016, p. 4).

A denúncia do MPF foi oferecida com base no art. 3º da Lei nº 13.260/16, após apenas 3 (três) meses da vigência da mesma no ordenamento jurídico brasileiro, circunstância que, pela primeira vez a Lei Antiterror foi empregada.

De acordo com Lehfeld, Nunes e Silva, se o grupo realizasse o ataque terrorista, esse ofenderia diretamente a Constituição Federal (CF), sendo:

Imperioso destacar que o desejado pelo grupo criminoso resultaria em ofensa principalmente a Constituição Federal, pois repulsa o terrorismo. Em segundo plano, atingiria a sociedade brasileira como um todo, pois escolha de possíveis alvos civis com base em preconceitos/estereótipos implicaria uma afronta a diversidade cultural, social e religiosa da qual o Brasil é demasiadamente abundante. (LEHFELD; NUNES e SILVA, 2020, p. 20).

O magistrado responsável pelo julgamento do caso, condenou os 8 (oito) denunciados, fundamentando-se na Lei nº 13.260/2016, por integração de

organização terrorista e ato preparatório, conforme artigos 3º e 5º da Lei Antiterror. Além dessa condenação, houve reconhecimento de prática de crime previsto na Lei nº 12.850/2013, por ocorrência de crimes de organização criminosa. Também houve condenação com base na Lei nº 7.716/89 por ato de racismo. Outra condenação encontrou fundamento na Lei nº 7.170/83, por propaganda de perseguição religiosa. Por fim, a sentença reconheceu práticas de crimes da Lei nº 2.889/56, por genocídio, da Lei nº 8.069/90, por corrupção de menor, tendo em vista que as investigações identificaram um menor de idade como integrante do grupo.

Desta forma, a Operação Hashtag foi considerada um marco do terrorismo no Brasil, na qual restou clara evidente que o país não estaria imune às ações de grupos terroristas, tampouco aos ataques terroristas em solo brasileiro. Aliás, com a realização dessa operação, houve um receio nos modos de prevenção dos ataques terroristas no país.

Uma vez abordado o conceito, os modos de agir e os principais grupos terroristas, a pesquisa avançara no seu fio condutor, buscando analisar a resposta jurídica brasileira em razão das ameaças terroristas.

3 FUNDAMENTOS DOUTRINÁRIOS E LEGISLATIVOS SOBRE AS PENALIDADES ACERCA DOS ATOS TERRORISTAS

O ordenamento jurídico brasileiro não possuía específica atenção com crimes de terrorismo, motivo pelo qual se observa uma enorme carência em relação às tipificações dos atos terroristas.

No Brasil, para disciplinar o terrorismo, foi criada a Lei nº 13.260/2016, denominada lei antiterrorismo, a qual trata da tipificação, julgamento e punições para os crimes que possuem natureza terrorista em território brasileiro. A referida legislação regulamenta o disposto no art. 5º, inciso XLIII da Constituição Federal.

O terrorismo é vetusto, aprimorando-se cada vez mais com o passar do tempo, no entanto o estudo aprofundado do tema é recente, tendo início apenas no século XX, possuindo maior visibilidade com a ocorrência de ataques terroristas. No Brasil havia uma ilusória intuição de que o país é isento de atos terroristas, desatentando-se de fundamentos doutrinários e legislativos com relação as penalidades dessa modalidade de crime.

A Constituição Federal de 1988, abordou de forma concisa o tema terrorismo, inserindo-o no título de garantias e direitos fundamentais. O art. 4º da CF faz menção direta ao terrorismo, o qual versa sobre regência do país em suas relações internacionais:

Art. 4º. A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: [...] VIII – repúdio ao terrorismo e ao racismo”. (Constituição Federal, 1988).

No art. 5º da Constituição Federal de 1988, encontra-se expresso que o terrorismo deverá ser equiparado a crime hediondo, desta maneira deverá ser insuscetível de graça ou anistia e inafiançável:

Art. 5º. [...]: XLIII – a lei considerará crimes inafiançáveis e insuscetíveis de graça ou anistia a prática de tortura, o tráfico ilícito de entorpecentes e drogas afins, o terrorismo e os definidos como crimes hediondos, por eles respondendo os mandantes, os executores e os que, podendo evitá-los, se omitirem”.

A Lei nº 8.930/94, deu nova redação ao art. 1º da Lei nº 8.072/90. O art. 1º define os crimes com caráter de hediondos, não fazendo menção ao

terrorismo, motivo pelo qual este é tido como equiparado a crime hediondo. Estabelece expressamente o art. 1º que:

"Art. 1º São considerados hediondos os seguintes crimes, todos tipificados no Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, consumados ou tentados:

I - homicídio (art. 121), quando praticado em atividade típica de grupo de extermínio, ainda que cometido por um só agente, e homicídio qualificado (art. 121, § 2º, I, II, III, IV e V);

II - latrocínio (art. 157, § 3º, **in fine**);

III - extorsão qualificada pela morte (art. 158, § 2º);

IV - extorsão mediante sequestro e na forma qualificada (art. 159, **caput**, e §§ 1º, 2º e 3º);

V - estupro (art. 213 e sua combinação com o art. 223, **caput** e parágrafo único);

VI - atentado violento ao pudor (art. 214 e sua combinação com o art. 223, **caput** e parágrafo único);

VII - epidemia com resultado morte (art. 267, § 1º).

Parágrafo único. Considera-se também hediondo o crime de genocídio previsto nos arts. 1º, 2º e 3º da Lei nº 2.889, de 1º de outubro de 1956, tentado ou consumado."

Para fins de normas processuais e de execução penal, o terrorismo submete-se aos mesmos tratamentos dos crimes considerado hediondos, versando sobre isso o art. 2º da Lei nº 8.072/90:

Art. 2º. Os crimes hediondos, a prática da tortura, o tráfico ilícito de entorpecentes e drogas afins e o terrorismo são insuscetíveis de: I – anistia, graça e indulto; § 1º A pena por crime previsto neste artigo será cumprida inicialmente em regime fechado. § 3º Em caso de sentença condenatória, o juiz decidirá fundamentadamente se o réu poderá apelar em liberdade. (Redação dada pela Lei nº 11.464, de 2007); § 4º A prisão temporária, sobre a qual dispõe a Lei nº 7.960, de 21 de dezembro de 1989, nos crimes previstos neste artigo, terá o prazo de 30 (trinta) dias, prorrogável por igual período em caso de extrema e comprovada necessidade. (Incluído pela Lei nº 11.464, de 2007).

Para NUCCI, embora o terrorismo não sendo um crime hediondo e sim equiparado a este, os atos são, em sua essência ainda mais hediondos do que os crimes mencionados:

A tortura, o tráfico ilícito de entorpecentes e o terrorismo somente não são considerados hediondos – embora sejam igualmente graves e repugnantes – porque o constituinte, ao elaborar o art. 5º, XLIII, CF, optou por mencioná-los expressamente como delitos insuscetíveis de fiança, graça e anistia, abrindo ao legislador ordinário a possibilidade de fixar uma lista de crimes hediondos, que teriam o mesmo tratamento. Assim, essas três modalidades de infrações são, na essência, tão ou mais hediondas que os crimes descritos no rol do art. 1º da Lei 8.072/90. (NUCCI, 2008, p.600).

De acordo com Silva, com a inclusão do terrorismo no texto constitucional de 1988, resultou na redemocratização da abertura de política do País, modificando também o conceito de segurança nacional, de modo que:

A inovação foi criada somente em 1988, a atual Constituição Federal, que se referiu expressamente ao terrorismo, enquadrando-o no âmbito das relações internacionais que o país deve manter com outros países. Foi a redemocratização quem trouxe abertura política do país e mudou o conceito de segurança nacional. O texto constitucional de 88, além de referir-se indiretamente ao terrorismo por duas vezes, refere-se diretamente ao assunto, tratando deste inclusive com destaque, inserindo disposições acerca do tema entre as cláusulas pétreas. (SILVA, 2010, p. 6).

O terrorismo possui previsão expressa na Constituição Federal de 1988, bem como na Lei nº 13.260/2016, a qual trata da tipificação do crime de terrorismo. Entretanto, o país não possuía uma política criminal especial acerca dos atos terroristas.

Por sua vez, na legislação brasileira, o ciberterrorismo se apresenta com maior destaque, pois conforme aludido por Alves e Barbosa “é notório a facilidade de obter dados e encontrar lacunas virtuais, o que estimula ações maiores que atinjam grupos maiores de pessoas” (ALVES e BARBOSA, 2021).

O ciberterrorismo é uma ramificação do cibercrime, sendo que no Brasil há alguns dispositivos que tratam dessa forma de crime, como a Lei Carolina Dieckmann e o Código Penal, no artigo 154 – A.

Merece nota, que o Brasil é um dos países que compõem a Lei Geral de Proteção de Dados (LGPD), a qual é assegurada e fiscalizada pela Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pelo cumprimento da LGPD no país.

3.1 ANÁLISE DA LEI 13.260/2016 – LEI ANTITERRORISMO

A Lei nº 13.260/2016 surgiu como um complexo normativo que tipificou o terrorismo e foi originada do Projeto de Lei da Câmara de nº 2016, de 2015, surgindo da iniciativa da Presidente da República, estabelecendo diversos crimes relacionados ao terrorismo, em regime de urgência. A referida lei busca sanções para os atos de terror praticados pelas organizações terroristas.

A Lei Antiterror se inseriu no campo do Direito Penal de Terceira Velocidade, incluindo-se no movimento de expansão do Direito Penal, o qual foi desenvolvido por Jesús-Maria Silva Sánchez, criando a Teoria das Velocidades do Direito Penal.

Sánchez *apud* Garcez, divide o Direito Penal em três velocidades, sendo a primeira velocidade:

O Direito Penal de Primeira Velocidade ficou caracterizado pelo respeito às garantias constitucionais clássicas, tendo em vista a aplicação da pena privativa de liberdade. Trata-se do modelo penal clássico, no qual o direito penal vem representado pela prisão, sem relativização das garantias processuais do imputado. Gize-se que o Estado responde ao crime de forma mais lenta, observando todos os mandamentos do devido processo legal, mas visa o encarceramento do criminoso ao final do processo penal.

O Direito Penal de Segunda Velocidade se caracterizou pela substituição da pena privativa de liberdade por penas alternativas. O estado abre mão aplicar ao infrator a pena de prisão, porém estabelece a relativização de garantias do imputado, i.e, opta-se por aplicar penas restritivas de direitos ou pecuniárias, mas, em contrapartida, determina a flexibilização das regras do direito penal clássico, proporcional à menor intensidade da sanção. Anote-se que o Estado responde ao crime de forma mais rápida, mas abdica do cárcere.

O Direito Penal de Terceira Velocidade, ao qual referimos que se insere a lei em estudo, ficou marcado pelo resgate da pena privativa de liberdade e pela manutenção da flexibilização de garantias do imputado. Trata-se de uma mescla das velocidades anteriores, sendo um modelo guiado pelos fundamentos do direito penal máximo. Esse modelo abarca o Direito Penal do Inimigo. O Estado responde ao crime de forma rápida e intensa, visando a submissão do imputado ao cárcere e restringindo suas garantias. (SÁNCHEZ, *apud* GARCEZ, 2021 p. 1398).

Ademais, Garcez registra uma Quarta Velocidade do Direito Penal na atualidade, a qual destina-se a quem violar de forma grave os tratados internacionais que versam sobre a tutela dos direitos humanos e, também para os Chefes de Estado. Essa Quarta Velocidade englobaria os casos que são julgados pelo Tribunal Penal Internacional, objetivando a aplicação de penas mais rígidas (GARCEZ, 2020, p. 1398).

O 1º artigo da Lei Antiterror regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, aduzindo que:

Art. 1º Esta Lei regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista.

O art. 2º, §1º da lei, estabelece quais os atos possíveis de caracterizar-se como crime de terrorismo, mostrando que se trata de condutas de variadas formas:

§ 1º São atos de terrorismo:

I - usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa;

II - (VETADO);

III - (VETADO);

IV - sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento;

V - atentar contra a vida ou a integridade física de pessoa:

Pena - reclusão, de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência.

Já o disposto no §2º do art. 2º, reporta-se de forma indireta às ações individuais, estipulando que não deve ser observado o que se encontra prescrito em tal artigo:

Art. 2º, § 2º O disposto neste artigo não se aplica à conduta individual ou coletiva de pessoas em manifestações políticas, movimentos sociais, sindicais, religiosos, de classe ou de categoria profissional, direcionados por propósitos sociais ou reivindicatórios, visando a contestar, criticar, protestar ou apoiar, com o objetivo de defender direitos, garantias e liberdades constitucionais, sem prejuízo da tipificação penal contida em lei.

Como visto, o caput do mesmo artigo faz menção às questões teleológicas, sendo essa uma das maiores motivações para a realização de atos terroristas, como aludido por CALLEGARI, LIRA, REGHELIN, MELIÁ e LINHARES, a intensificação de imigrantes em alguns países, pode acarretar a insatisfação de certos grupos religiosos, motivando-os a realização de ações terroristas (CALLEGARI; LIRA; REGHELIN; MELIÁ; e LINHARES, 2016, p.95).

Salienta-se, por oportuno, que as manifestações sociais não são consideradas atos terroristas, desde que não apresentem os componentes que se caracterizem como terrorismo, além de não ter como finalidade aterrorizar às

pessoas. Desta forma, não é cabível aplicar as sanções destinadas aos atos terroristas em desfavor das manifestações sociais, conforme expresso pelo art. 2º, §2º, da Lei 13.260/2016.

Ademais, salienta-se o crime de dupla subjetividade passiva no art. 2º desta lei, uma vez que possui pluralidade de vítimas para configuração do crime de terrorismo, devendo o ato ser praticado contra mais de apenas um indivíduo.

O art. 3º desta lei está voltada para aquele que possui de alguma forma, ligação com uma organização terrorista, deve-se ressaltar, que a pena imposta nesse artigo é inferior à do art. 2º:

Art. 3º Promover, constituir, integrar ou prestar auxílio, pessoalmente ou por interposta pessoa, a organização terrorista:
Pena - reclusão, de cinco a oito anos, e multa.

O artigo em questão, possui a natureza jurídica de um crime de perigo abstrato, tendo em vista que será aplicada a punição quando houver concretização de dano ao bem jurídico de qualquer indivíduo.

O art. 5º se direciona aos atos preparatórios, caracterizando a punição destes como:

Art. 5º Realizar atos preparatórios de terrorismo com o propósito inequívoco de consumir tal delito:
Pena - a correspondente ao delito consumado, diminuída de um quarto até a metade.

No artigo mencionado, verifica-se a existência de punição para os atos preparatórios relacionados ao terrorismo, os quais, via de regra, não são punidos pelo ordenamento jurídico brasileiro nos demais crimes. Entretanto, na Lei 12.360/2016, constatou-se uma necessidade de aplicar uma punição para tais atos, podendo utilizar como exemplo a troca de mensagens via celular, objetivando realizar a execução de um ato terrorista. Ademais, a punição trazida neste artigo, incide diretamente no Direito Penal do Inimigo, na versão teórica de Günter Jakobs.

O §1º do mesmo artigo, faz menção à previsão de quem incorre na mesma pena aplicada no caput do artigo, sendo:

§ 1º Incorre nas mesmas penas o agente que, com o propósito de praticar atos de terrorismo:

I - recrutar, organizar, transportar ou municiar indivíduos que viajem para país distinto daquele de sua residência ou nacionalidade; ou
II - fornecer ou receber treinamento em país distinto daquele de sua residência ou nacionalidade.

Já o §2º refere-se à punição para o terrorismo considerado interno, ou seja, aquele que ocorre dentro do País:

§ 2º Nas hipóteses do § 1º, quando a conduta não envolver treinamento ou viagem para país distinto daquele de sua residência ou nacionalidade, a pena será a correspondente ao delito consumado, diminuída de metade a dois terços.

O 6º artigo da Lei 13.260/2016, faz alusão ao financiamento do terrorismo:

Art. 6º Receber, prover, oferecer, obter, guardar, manter em depósito, solicitar, investir, de qualquer modo, direta ou indiretamente, recursos, ativos, bens, direitos, valores ou serviços de qualquer natureza, para o planejamento, a preparação ou a execução dos crimes previstos nesta Lei:

Pena - reclusão, de quinze a trinta anos.

Parágrafo único. Incorre na mesma pena quem oferecer ou receber, obtiver, guardar, mantiver em depósito, solicitar, investir ou de qualquer modo contribuir para a obtenção de ativo, bem ou recurso financeiro, com a finalidade de financiar, total ou parcialmente, pessoa, grupo de pessoas, associação, entidade, organização criminosa que tenha como atividade principal ou secundária, mesmo em caráter eventual, a prática dos crimes previstos nesta Lei.

O 7º artigo, elenca as causas de aumento da pena de acordo com o resultado de determinadas condutas terroristas:

Art. 7º Salvo quando for elementar da prática de qualquer crime previsto nesta Lei, se de algum deles resultar lesão corporal grave, aumenta-se a pena de um terço, se resultar morte, aumenta-se a pena da metade.

Neste artigo, pode-se apontar uma eventual falha do legislador no tocante à incidência da majorante, pois se deveria levar em conta a quantidade de mortes, uma vez que determinada conduta resultar em muitas mortes, será aplicável a fração de 1/3 ou de metade. Assim, caberá ao juiz analisar o número de mortes, para realizar a dosagem da pena.

Por sua vez, o artigo 10º refere-se às penas aplicadas nos casos de desistência voluntária e arrependimento eficaz:

Art. 10. Mesmo antes de iniciada a execução do crime de terrorismo, na hipótese do art. 5º desta Lei, aplicam-se as disposições do art. 15 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal.

Nos crimes em que se punem os atos preparatórios, é possível que o sujeito alcançado pelo arrependimento eficaz e desistência voluntária, ainda que não tivesse iniciado a execução deste.

Com relação ao regime inicial de cumprimento da pena no crime de terrorismo, tendo em vista que o mesmo é equiparado a hediondo, deverá se observar de forma cumulativa o disposto no art. 33, §3º e o disposto no art. 59, ambos do Código Penal.

O 18º artigo da lei informa que a redação do art. 1º da Lei nº 7.960 de 1989, passou a vigorar com o acréscimo da alínea p sendo:

Art. 18. O inciso III do art. 1º da Lei nº 7.960, de 21 de dezembro de 1989, passa a vigorar acrescido da seguinte alínea p :
 “Art. 1º

 III -

 p) crimes previstos na Lei de Terrorismo.” (NR)

Merece nota o fato de, que a Lei nº 7.960 versa sobre a prisão temporária ao dispor que, quando houver qualquer razão fundada e lícita de que o indivíduo tenha autoria ou participação em um ato que se configure terrorismo, poderá ser aplicada a prisão temporária do mesmo.

Contudo, deve-se ressaltar, que a prisão temporária será aplicada com base no disposto artigo 2º, §4º da Lei nº 8.072/90, de forma que:

Art. 2º Os crimes hediondos, a prática da tortura, o tráfico ilícito de entorpecentes e drogas afins e o terrorismo são insuscetíveis de:
 (Vide Súmula Vinculante)

I - anistia, graça e indulto;

II - fiança e liberdade provisória.

II - fiança. (Redação dada pela Lei nº 11.464, de 2007)

§ 1º A pena por crime previsto neste artigo será cumprida integralmente em regime fechado.

§ 1o A pena por crime previsto neste artigo será cumprida inicialmente em regime fechado. (Redação dada pela Lei nº 11.464, de 2007)

§ 2º Em caso de sentença condenatória, o juiz decidirá fundamentadamente se o réu poderá apelar em liberdade.

§ 2o A progressão de regime, no caso dos condenados aos crimes previstos neste artigo, dar-se-á após o cumprimento de 2/5 (dois quintos) da pena, se o apenado for primário, e de 3/5 (três quintos), se reincidente. (Redação dada pela Lei nº 11.464, de 2007)

§ 2º A progressão de regime, no caso dos condenados pelos crimes previstos neste artigo, dar-se-á após o cumprimento de 2/5 (dois quintos) da pena, se o apenado for primário, e de 3/5 (três quintos), se reincidente, observado o disposto nos §§ 3º e 4º do art. 112 da Lei nº 7.210, de 11 de julho de 1984 (Lei de Execução Penal). (Redação dada pela Lei nº 13.769, de 2018) (Revogado pela Lei nº 13.964, de 2019)

§ 3º A prisão temporária, sobre a qual dispõe a Lei nº 7.960, de 21 de dezembro de 1989, nos crimes previstos neste artigo, terá o prazo de trinta dias, prorrogável por igual período em caso de extrema e comprovada necessidade.

§ 3o Em caso de sentença condenatória, o juiz decidirá fundamentadamente se o réu poderá apelar em liberdade. (Redação dada pela Lei nº 11.464, de 2007)

§ 4o A prisão temporária, sobre a qual dispõe a Lei no 7.960, de 21 de dezembro de 1989, nos crimes previstos neste artigo, terá o prazo de 30 (trinta) dias, prorrogável por igual período em caso de extrema e comprovada necessidade. (Incluído pela Lei nº 11.464, de 2007).

Desta maneira, nota-se que o prazo máximo é de trinta dias, prorrogáveis somente uma única vez por mais trinta dias, não se aplicando neste caso o prazo máximo de cinco dias.

Ao cabo, como já referido o crime de terrorismo é equiparado a hediondo, não havendo dúvida sobre a equiparação do art. 2º a de crime hediondo, tendo em vista que o crime de terrorismo exige um especial motivo para agir e um especial fim, sendo esses elementos especiais além do dolo. Ademais, deve-se demonstrar as razões para a prática de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião.

3.2 CARÊNCIA DO CÓDIGO PENAL EM RELAÇÃO AO CRIME DE (NEO)TERRORISMO

Conforme já analisado anteriormente, no Brasil, o crime de terrorismo está expresso no art. 4º da Constituição Federal e tipificado na Lei nº 13.260/2016, no entanto o Código Penal brasileiro apresenta lacuna quando o assunto é o crime de terrorismo, uma vez que grande parte do governo adere uma conduta de “negacionismo”, no tocante a negar a existência de qualquer tipo de atividade terrorista no País.

Para Silva, as preocupações com o crime de terrorismo somente entram em destaque, após a realização de ataques terroristas, sendo que:

Embora o terrorismo seja fenômeno tão antigo quanto a civilização humana, seu estudo pela doutrina jurídica tem menos de um século e a sua discussão só aparece com mais força quando atentados ocorrem. Sendo assim, percebe-se que as providências contra o terror são imediatistas, olvidando-se reais ações preventivas, em detrimento de medidas paliativas pós-ataque. Na verdade, o incremento constante do terror revela a necessidade de uma abordagem que vá além da discussão meramente superficial. (SILVA, 2010, p.1).

Conforme mencionado por Lasmar:

Em realidade, o terrorismo internacional tem sido uma preocupação da Polícia Federal desde o início da década de 1980. Os atentados à embaixada e quartéis estadunidenses em Beirute, em 1983, suscitou a preocupação no governo brasileiro de que sequestros de aeronaves e atentados a bomba pudessem vir a ocorrer no Brasil. Essa preocupação foi real o suficiente para levar a que uma Comissão Parlamentar Mista de Inquérito recomendasse ao Ministério da Justiça a criação de um grupo especializado em contraterrorismo. Esse grupo começou a operar alguns anos mais tarde se tornando o Comando de Operações Táticas (COT) da Polícia Federal. O COT se encontra ativo até os dias de hoje e ainda tem como uma de suas competências a resposta cinética a atos de terrorismo. (LASMAR, 2015).

Prosseguindo Silva, refere que:

Pesquisando como o terrorismo se manifestou na história do Brasil, verifica-se que a raiz do terror no país é frequentemente relacionada à ditadura militar de 1964, quando, em 31 de março, setores militares apoiados pelos EUA e por segmentos da sociedade civil brasileira depuseram o então presidente João Goulart, dando início ao período que marcou para sempre a história do país. Com o Ato Institucional nº

5, de 13 de dezembro de 1968 (AI-5), o regime militar endureceu-se ainda mais, desenvolvendo uma fase de intensa repressão e de caça aos brasileiros considerados “subversivos” pela nova regra. (SILVA, 2010, p.3).

Dessa forma, ainda que o terrorismo esteja expresso em texto constitucional, tal regramento não possui um instrumento normativo infraconstitucional sobre a temática do terror, uma vez que não foi apropriada a uma legislação penal correspondente (SILVA, p.2, 2010). De acordo com a legislação europeia, o Decreto nº 4.269 de 1921 e a Lei nº 38, de 1935, foram os primeiros dispositivos sobre a temática, prevendo punições para os autores de crimes contra ordem pública (SILVA, p. 8, 2010).

Com relação ao ciberterrorismo, Barbosa e Alves mencionam que:

[...]sabendo que o ciberterrorismo é uma extensão do terrorismo e uma especificação do cibercrime, é válido toda e qualquer forma de prevenção contra tais práticas, visto que não são todos os ordenamentos que preveem essa dinâmica ilícita virtualmente, assim como o Brasil também não desenvolveu medidas específicas dessa forma necessária. (BARBOSA e ALVES, 2021).

Verifica-se, portanto, que o Código Penal possui artigos específicos para tratar de invasões de sistemas de outros usuários, conforme expresso pelo art. 154 - A:

Art. 154-A. Invasão de dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021).

Ademais, o §1º do mesmo artigo aduz sobre as demais possibilidades de inclusão no art. 154 – A, enquanto o §2º versa sobre o aumento de pena:

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012) Vigência

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021).

Já o §3º do art. 154 – A refere sobre a possibilidade de obtenção de conteúdos privados e sigilosos:

§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021).

Por sua vez, os §4º e 5º, mencionam a hipótese de aumento da pena em determinadas situações:

§ 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (Incluído pela Lei nº 12.737, de 2012) Vigência

§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência

I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência

II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012) Vigência

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012) Vigência

Ação penal (Incluído pela Lei nº 12.737, de 2012) Vigência.

Agnoletto e Bezerra fazem algumas considerações gerais sobre o art. 154 – A do Código Penal:

Trata-se de infração de menor potencial ofensivo, portanto, a competência para julgamento de eventual crime será do Juizado Especial Criminal (Art. 61 da Lei 9.099/95). Em princípio, consoante regra prevista no Art. 69 da Lei 9.099/95, a investigação deverá ser feita através da lavratura de Termo Circunstanciado, entretanto, a complexidade na apuração da autoria e materialidade do delito de

invasão de dispositivo informático, que muitas vezes irá demandar requisição de dados cadastrais, perícia em computadores, busca e apreensão, interrogatórios de testemunhas, etc, provavelmente ensejará a instauração de Inquérito Policial.

Consumação: por tratar-se de crime formal, consuma-se com a invasão.

Sendo assim, a obtenção, adulteração ou destruição de dados ou a instalação de vulnerabilidades serão mero exaurimento do delito informático “invasão de dispositivo”.

Tentativa: Admite-se a tentativa. Ex. agente inicia os atos executórios para invasão do equipamento (computador), todavia, por razões alheias a sua vontade, não consegue violar os dispositivos de segurança.

Pena: A pena para o delito informático previsto no “caput” do Art. 154-A (detenção de 03 meses a 01 ano, e multa) é baixa, apresentando mais um componente de caráter psicológico para a prevenção do crime do que uma efetiva punição ao autor. (AGNOLETTO e BEZERRA, 2020, p. 27).

Barbosa e Silva mencionam a importância da aplicação do Direito Penal em face do ciberterrorismo:

Do ponto de vista indutivo, nota-se que muitas pessoas não cometeriam crimes nas relações reais, ou seja, pessoa x pessoa, porém no ciberespaço encontrarão a segurança de cometer crimes, seja pela forma direta de crime como fraude ou pelo uso de meios como o virtual, exemplo tráfico de drogas. O direito penal é visto como a razão final, ou seja, é preciso buscar todos os outros meios antes de recorrer a esse ramo. Nesse sentido, diante das mudanças sociais, os crimes cibernéticos têm se tornado cada vez mais comuns e despertam algumas suspeitas quando aparecem. Nessa perspectiva, considerando que a lei deve ser efetiva, é importante entender como o direito penal se aplica diante do crime cibernético. Ou seja, se as normas do direito penal não são aplicáveis, não há necessidade de tipificá-las. (BARBOSA e SILVA, 2021).

Como visto, embora tenha sido aprovada e sancionada a Lei Antiterror, é possível sustentar ainda uma debilidade na política criminal do País em relação à normatização de condutas consideradas com (neo)terrorismo. Essa conclusão advém da constatação da pesquisa de que no sistema penal atual, não há menção, de forma direta, o (neo)terrorismo antigo, ao contrário da Constituição Federal e da Lei Antiterror (Lei nº 13.260/2016). Já com relação ao ciberterrorismo, esse possui um maior destaque no Código Penal, tendo em vista o disposto no artigo 154 – A e parágrafos, os quais estipulam às hipóteses de crime e suas respectivas penas.

CONCLUSÃO

O presente estudo abordou a contextualização do (neo)terrorismo: ameaças cibernéticas e a racionalidade da lei penal, a partir do contexto histórico, social e jurídico. Buscou-se, como objetivos delimitar o trabalho na análise do surgimento deste novo terrorismo, nos métodos utilizados para realizar os ataques terroristas, nas formas de disseminação das ideologias e políticas dos grupos terroristas. Além disso, aprofundou-se no estudo da utilização do ciberterrorismo como uma das formas de operação do (neo)terrorismo e analisou a carência da legislação penal acerca da temática.

A expansão do (neo)terrorismo possui reflexos diretos e indiretos no crescimento das ações radicais de grupos terroristas, visando a utilizar a política criminal do processo de racionalidade da lei penal brasileira como uma resposta jurídica à expansão dos crimes cibernéticos.

Não há como definir um único conceito para terrorismo, uma vez que a temática é multifacetada e complexa, além de estar ligada diretamente ao cenário atual vivenciado, motivo pelo qual há grande divergência nos conceitos de terrorismo. Contudo, verifica-se que todas as conceituações englobam a utilização de atos criminosos que empregam a violência e o medo para controlar e amedrontar seus alvos, podendo sua motivação estar relacionado a questões política, religiosas ou ideológicas.

O ciberterrorismo, por sua vez, possui uma conceituação mais direta e simples, apesar de também não possuir um único conceito. O terrorismo cibernético pode ser definido como ações realizadas a partir de aparelhos eletrônicos, fazendo o uso da internet em grande parte dos ataques, os quais atingem de forma rápida e quase sempre imperceptível as redes computacionais de informação, podendo causar-lhes uma incapacitação temporária ou a destruição total.

O velho terrorismo surge no século III, a.C, como uma das inúmeras táticas empregadas pelos militares visando seus objetivos como as vitórias em guerra e o recebimento do apoio da população. Por sua vez, o (neo)terrorismo surge após a revolução francesa, no século XIX, reestruturando o antigo terrorismo e trazendo um novo “modus operandi” na realização dos atentados. Os ataques realizados em 11 de setembro de 2001, podem ser considerados

como o marco inicial do novo terrorismo, além de destinar grande protagonismo aos principais grupos terroristas da atualidade. Necessário salientar, que o terrorismo e a guerra são ações completamente distintas, possuindo como uma das principais diferenças, a sua finalidade individual.

Embora o fenômeno do terrorismo seja conhecido em boa parte do mundo, sobretudo na América do Norte, Europa, Oriente Médio e África, no Brasil, o mais expoente – e, talvez, o único – ato terrorista aconteceu com o desencadeamento da Operação Hashtag, tida como um marco do (neo)terrorismo, retomando o problema dos ataques terroristas, na qual identificou a partir de mensagens por redes sociais, a realização de um possível ataque terrorista durante as olimpíadas de 2016, sendo esse organizado pelo grupo denominado como “Defensores de Sharia”, composto por brasileiros que possuíam ligação com membros do Estado Islâmico.

O terrorismo utiliza meios cruéis e mortíferos para a realização de ataques, tendo como motivação razões pessoais, ligadas a fatores políticos, religiosos e sociais, tendo como finalidade a punição de seus inimigos/alvos. Já a guerra, possui cunho social, visando combater alvos que possam ou estão ameaçando o Estado e a população como um todo.

O (neo)terrorismo expandiu-se de maneira quase incoercível, principalmente nos avanços relacionados aos meios de comunicação e a ampliação da rede mundial de computadores. O aperfeiçoamento dos aparelhos eletrônicos e da internet resultou na evolução dos novos tipos de ameaças cibernéticas como, o Phishing, o Hacking, o Spam entre vários outros. Desta forma, o ciberterrorismo tornou-se um dos principais “modus operandi” do novo terrorismo, tendo em vista sua eficácia, segurança e baixo custo, bem como o seu alto grau de impacto e destruição nos alvos selecionados.

As hipóteses do presente trabalho, se delimitaram em analisar racionalidade da lei penal brasileira, a qual sofre com a expansão do (neo)terrorismo, tendo em vista a extrema carência do Código Penal em relação ao (neo)terrorismo, sendo que não possui nenhuma previsão expressa em seus artigos sobre esse crime. O crescimento dos meios de propagação dos ataques terroristas, principalmente às ameaças cibernéticas afetam a racionalidade da lei penal, uma vez que essa é desprovida de dispositivos que regulamentem a temática em questão.

A Lei 13.260/2016 (Lei Antiterror), foi elaborada exclusivamente para tipificar e definir o terrorismo, além de estabelecer penalidades aos praticantes de atos terroristas. Entretanto, o Direito Penal não se mostra absolutamente eficaz para prevenir e reprimir as novas práticas terroristas cibernéticas.

O (neo)terrorismo e as ameaças cibernéticas carecem de um estudo mais aprofundado, capaz de identificar as raízes dos atos terroristas, bem como um método para frear a expansão do ciberterrorismo, desenvolvendo formas eficazes e seguras de prevenir ataques. Ademais, é necessário regulamentar outros dispositivos que aduzam sobre a prática do novo terrorismo, utilizando-se as ameaças cibernéticas, as quais visam atingir seus alvos causando o maior nível de danificação possível e, ou sua destruição total.

A pesquisa realizada foi capaz de demonstrar a carência da lei penal brasileira em relação ao (neo)terrorismo e as ameaças cibernéticas, ressaltando conceitos importantes, identificando o aperfeiçoamento do ciberterrorismo como “*modus operandi*”, além de destacar que o País não está totalmente livre da possibilidade de realização de atos terroristas.

Ao cabo, é visível que o (neo)terrorismo teve uma enorme expansão no século XXI, a qual resultou na aprimoração de seus “*modus operandi*”, optando por meios de ataques que fossem mais rápidos e eficazes como, as ameaças cibernéticas. No entanto, o Direito Penal brasileiro não evoluiu no mesmo nível que o (neo)terrorismo, deixando lacunas que precisam ser preenchidas com o intuito de prevenir e penalizar os ataques terroristas, motivo pelo qual é necessário buscar formas de repressão aos atentados, minimizando as ações dos grupos terroristas.

REFERÊNCIAS

AGNOLETTO, Giovani Celso; BEZERRA, Clayton da Silva. **Combate ao crime cibernético**. 1. ed.- Rio de Janeiro; Mallet e Editora, 2020.

ALCÂNTARA, Bruna Toso de. **Internet, Terror e Ciberterrorismo: uma análise comparativa**, 2018. Disponível em: <<https://lume.ufrgs.br/bitstream/handle/10183/182448/001076042.pdf?sequenc e=1&isAllowed=y>>. Acesso em 07 de mai. 2022.

ALVES, Ana Beatriz de Oliveira; BARBOSA, Rebeca Laiza Nascimento. **Cibercrime e ciberterrorismo: Até que ponto a ausência de segurança cibernética contribui para as práticas terroristas**, 2021. Disponível em: <<https://jus.com.br/artigos/89044/cibercrime-e-ciberterrorismo-ate-que-ponto-a- ausencia-de-seguranca-cibernetica-contribui-para-as-praticas-terroristas>>. Acesso em 11 de jun. 2022.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro, dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em. 14 de mai. 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 14 de mai. 2022.

BRASIL. Denúncia, de 15 de setembro de 2016. Ministério Público Federal. **Operação Hashtag**, 2016. Disponível em: <<http://www.mpf.mp.br/pr/sala-de- imprensa/docs/DennciaOperacaoHashtag.pdf/view>>. Acesso em: 15 de jun. 2022.

BRASIL. **Lei nº 2.889**, de 1º de outubro de 1956. Define e pune o crime de genocídio. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l2889.htm>. Acesso em 03 de dez. 2021.

BRASIL. **Lei nº 7.960**, de 21 de dezembro de 1989. Dispõe sobre prisão temporária. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7960.htm>. Acesso em 14 de mai. 2022.

BRASIL. **Lei nº 8.072**, de 25 de julho de 1990. Dispõe sobre os crimes hediondos, nos termos do art. 5º, inciso XLIII, da Constituição Federal, e determina outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8072.htm>. Acesso em 14 de mai. 2022.

BRASIL. **Lei nº 13.260**, de 16 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis nº 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm>. Acesso em 14 de mai. 2022.

BRASIL. **Sentença Operação Hashtag**, 2017. Operação Hashtag. Disponível em: <<https://www.conjur.com.br/dl/presos-operacao-hashtag-sao-condenados.pdf>>. Acesso em 28 de mai. 2022.

BAPTISTA, Ricardo Córdoba. **O que é ciberterrorismo**. Copyright© MyCyberSecurity. Disponível em: <<https://www.mycybersecurity.com.br/author/mycyber/page/15/>>. Acesso em 20 de set.2021.

BARRETO, Eduardo Müssnich. **Terrorismo cibernético e cenários especulativos**. Revista Brasileira de Inteligência, 2007. Disponível em: <<https://rbi.enap.gov.br/index.php/RBI/article/view/59>>. Acesso em 20 de set. 2021.

BRAZ, Marcelo. **Saúde, Serviço Social, movimentos sociais e conselhos: desafios atuais**. 2ª. ed. [S.l.]: Cortês, 2012.

CABETTE, Eduardo Luiz Santos, NAHUR, Marcius Tadeu Maciel. **Terrorismo Lei 13.260/16** comentada, 2017.

CALLEGARI, André Luís; LIRA, Cláudio Rogério Sousa; REGHELIN, Elisangela Melo; MELIÁ, Manuel Cancio; e LINHARES, Raul Marques. **O Crime de Terrorismo**, 2016.

CHAGAS, Morgana Santos das. **Ciberterrorismo: As possibilidades da expansão do terror nas relações internacionais**, 2012. Disponível em: <<https://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/11089/1/PDF%20-%20Morgana%20Santos%20das%20Chagas.pdf>>. Acesso em 16 de abr. 2022.

COELHO, Werlan Carla Specemille Ressureição. **Neoterrorismo e a insuficiência dos instrumentos de controle do financiamento**, 2019. Disponível em: <<https://repositorio.uniceub.br/jspui/bitstream/prefix/14508/1/61450044.pdf>>. Acesso em: 16 de abr. 2022.

CRUZ, Danielle Maia; PEIXOTO, Fábio Carvalho de Alvarenga. **Terrorismo, Manifestações Sociais e Democracia: uma análise sobre a proposta de**

alteração da Lei nº 13.260/2016, 2019. Disponível em: <<https://seer.ufrgs.br/sociologias/article/view/96865/64110>>. Acesso em 03 de dez. 2021.

DINIZ, Eugenio. **Compreendendo o Fenômeno do Terrorismo**, 2002. Disponível em: <<https://ciberativismoeguerria.files.wordpress.com/2016/09/diniz-do-o-fenomeno-do-terrorismo.pdf>>. Acesso em 07 de mai. 2022.

DUDLEY, Dominc. **Os grupos terroristas que mais matam no mundo atualmente**, 2018. Revista Forbes. Disponível em: <<https://forbes.com.br/colunas/2018/12/os-grupos-terroristas-que-mais-matam-no-mundo-atualmente/>>. Acesso em 07 de mai. 2022.

GABINETE DAS NAÇÕES UNIDAS CONTRA A DROGA E A CRIMINALIDADE. **11º Congresso das Nações Unidas sobre Prevenção de Crime e Justiça Penal**. 2005. Bangucoque, Tailândia. Disponível em: <https://unis.unvienna.org/pdf/05-81509_S_1_SFS.pdf>. Acesso em 12 de mar. 2022.

GARGEZ, Willian. **Leis Penais Especiais Comentadas na visão do STF e STJ**, 2021. Editora Mizuno.

HOBBSWAN, Eric John Ernest. **A Era dos Impérios**, 1914, p. 288. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/4018951/mod_resource/content/1/A%20Era%20dos%20Imperios%201875-1914%20-%20Eric%20J.%20Hobsbawm.pdf>. Acesso em 07 de set. 2021.

HUDSON, Rex A. **The Sociology And Psychology of Terrorism: Who Becomes a Terrorist And Why?** Washington, D.C.: The Library of Congress, 1999. Disponível em: <https://www.loc.gov/rr/frd/pdf-files/Soc_Psych_of_Terrorism.pdf>. Acesso em 14 de nov. 2021.

LEITE, Igor dos Santos. **Os impactos da evolução do Terrorismo no cenário Global (pós 11/09 e Isis) e seus efeitos para o Brasil**, 2020. Disponível em: <<https://bdex.eb.mil.br/jspui/bitstream/123456789/8861/1/MO%206316%20-%20IGOR.pdf>>. Acesso em 16 de abr. 2022.

LEHFELD, Lucas Souza; NUNES, Danilo Henrique; SILVA, Jonatas Santos. **Ciberterrorismo e soberania: análise da operação Hashtag como ato atentatório ao Estado**, 2020. Disponível em: <<https://ojs.ufgd.edu.br/index.php/videre/article/view/11075/6296>>. Acesso em: 04 de jun. 2022.

LIMA, Renato Brasileiro. **Legislação Criminal Especial Comentada**. Salvador: Juspodivm, 2020, p. 952.

LIRA, Cláudio Rogério Sousa. **A Resposta ao Terrorismo pelo Direito: Um Crime Transnacional e de Natureza Jurídica de Tratado**, 2018. Disponível em: <http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/7476/CI%20c3%a1udio%20Rog%20Sousa%20Lira_.pdf?sequence=1&isAllowed=y>. Acesso em 20 de out. de 2021.

MELIÁ, Manuel Cancio. Los delitos de terrorismo: estrutura típica e injusto. Madrid: Editora Re.us, 2010, p. 70.

MD31-M-07, de 2017. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf>. Acesso em 12 de mar. de 2022.

MD35-G-01, de 2015. Disponível em https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em 13 de set. de 2021.

ONU. **Relatório da Organização das Nações Unidas**, de 2005. Disponível em <http://www.unric.org/pt/informacao-sobre-a-onu>. Acesso em 07 de set. de 2021.

PETERKE, S. **Obrigações internacionais para criminalização do terrorismo e modelos de implementação**. Principais opções para o legislador brasileiro. Revista de informação legislativa. Brasília. 2014.

PINTO, Marco Aurélio Gonçalves. **Teoria relativista do ciberterrorismo**. Dissertação para a obtenção do grau de Mestre em Guerra da Informação. Academia Militar. Lisboa, 2011. Disponível em: <https://comum.rcaap.pt/bitstream/10400.26/6826/1/Ciberterrorismo_tese_VersFinal.pdf>. Acesso em 21 de set. de 2021.

RAPOSO, Alisson Campos. **Terrorismo e contraterrorismo**. Revista Brasileira de Inteligência, Brasília, V.3, n.4, p 42-43, 2007.

SILVA, Francisca Jordânia Freitas da. **Tratamento penal do terrorismo no Brasil**, 2010. Disponível em: <https://www.uni7.edu.br/recursos/imagens/File/direito/ic2/vi_encontro/TRATAMENTO_PENAL_DO_TERRORISMO_NO_BRASIL.pdf>. Acesso em 04 de jun. 2022.

TANGERINO, Dayane Fanti. O papel do Estado no combate ao ciberterrorismo, 2016. Disponível em: <<https://canalcienciascriminais.com.br/o-papel-do-estado-no-combate-ao-ciberterrorismo/>>. Acesso em 14 de mai. 2022.

TEIXEIRA DA SILVA, Francisco Carlos. **O Brasil na crise internacional**. Texto apresentado no Simpósio “Análise e consequências do ato terrorista ocorrido

nos EUA, em 11 de setembro de 2001”. Escola de Guerra Naval, novembro de 2001.

VEIGA, Eduardo de Lima. **Terrorismo e Direito Penal do Inimigo: contornos e legitimidade à luz do Direito Internacional**. 2018.

WILKINSON, Paul. **Terrorismo político**. Rio de Janeiro: Editora Artenova, 1976, p. 19.

WITCKER, Ivan. **Occidente ante las nuevas tipologías del terrorismo**. Estudios Públicos, Santiago, Chile, n. 98, otoño 2005. Disponível em: <https://www.cepchile.cl/occidente-ante-las-nuevas-tipologias-delterrorismo/cep/2016-03-04/093633.html>. Acesso em 12 de set. 2021.

WOLOSZYN, A. L. **Aspectos gerais e criminais do terrorismo e a situação do Brasil**. Revista do Ministério Público (Rio Grande do Sul), 2005. Disponível em: <http://www.amprs.com.br/public/arquivos/revista_artigo/arquivo_1273861260.pdf>. Acesso em 15 de set. 2021.

WRIGHT, Lawrence. **O Vulto das Torres: A Al-Qaeda e o caminho até 0 11/09**. Revista Técnica Paulo Farah, editora Schwarcz Ltda, 2006.