Revista VIDERE
v. 12, n. 24
maio/agosto, 2020
p. 93 a 118
ISSN: 2177-7837

CIBERTERRORISMO E SOBERANIA: ANÁLISE DA OPERAÇÃO *HASHTAG* COMO ATO ATENTATÓRIO AO ESTADO

CYBERTERRORISM AND SOVEREIGNTY: ANALYSIS OF THE HASHTAG OPERATION AS AN ATTENTATORY ACT TO THE STATE

Danilo Henrique Nunes
Doutorando e mestre em Direitos Coletivos e Cidadania pela Universidade de Ribeirão Preto/SP (Unaerp), Brasil
Professor do Centro Universitário da Fundação Educacional de Barretos (UNIFEB), Brasil
E-mail: dhnunes@hotmail.com
OrcID: http://orcid.org/0000-0001-9162-3606

Lucas Souza Lehfeld
Doutor em Direito pela Pontifícia Universidade Católica de São Paulo (PUCSP), Brasil
Professor da Unaerp, Brasil
E-mail: lehfeldrp@gmail.com
OrcID: http://orcid.org/0000-0002-1021-0891

Jonatas Santos Silva
Especialista em Ciências Criminais pela Faculdade de Direito da Universidade de Ribeirão Preto/SP, Brasil
E-mail: jonatashet23@gmail.com
OrcID: http://orcid.org/0000-0002-7338-299X

RESUMO: Devido a expansão e progressão tecnológica, bem como o uso intenso da *Internet*, foi possibilitado o surgimento de diversos crimes praticados no âmbito virtual, tais como o ciberterrorismo. Desse modo, o presente artigo propõe, em síntese, um estudo acerca dos atos ciberterroristas, perfazendo uma análise de sua conceituação e atuação no âmbito virtual, seja na *Surface Web, Deep Web* ou *Dark Web* e, ainda, de como deverá ser aplicado o ordenamento jurídico brasileiro quando da incidência do referido crime. Ademais, destaca-se que esses ataques terroristas, um problema mundial que aparentava ser distante da realidade brasileira e que agora são passíveis de realização no ciberespaço, possuem o potencial de causar o pânico na sociedade, ameaçando, inclusive, o poder soberano de um Estado, tornando-os reféns do medo. Tendo em vista tais aspectos, será feita uma apreciação da legitimidade para aplicação da Lei Antiterrorismo (Lei nº 13.260/2016) de caráter excepcional, bem como um estudo de caso concreto da primeira aplicação efetiva da Lei. A problemática da nova realidade tecnológica será abordada mediante pesquisa exploratória que visa analisar uma real possibilidade de ataque ciberterrorista. O método de pesquisa utilizado é o bibliográfico, através de artigos, críticas e reflexões, ponderando seu impacto no Direito Penal vigente. Todavia, não se pode descartar a possível desestabilização do Estado em razão da propagação ao terror causado por essa cibercriminalidade, sendo necessária uma adequada abordagem devido ao grau de periculosidade, excepcionalidade e dimensão dos danos, com embasamento nos direitos fundamentais previstos na nossa Carta Magna.

Palavras-chave: Ciberterrorismo; *Internet*; *Deep Web;* Disseminação da ameaça.

ABSTRACT: Due to the expansion and technological progression, as well as the fierce use of the Internet, it has allowed the possibility of several crimes committed in virtual environment, such as cyber terrorism. Thus, this study proposes, in synthesis, a study about cyberterrorist acts, making an analysis of its conceptualization and performance in a virtual sphere, either on the Surface Web, Deep Web or Dark Web and also how it should be applied in the Brazilian legal system upon the crime said so. In addition, it is featured that these terrorist attacks, a world problem that seemed to be far from the Brazilian reality and now capable of being fulfilled out in cyberspace, have the potential to cause panic in society, threatening even the sovereignty power of the State, making them hostage to fear. In the view of these aspects, it will be made an appreciation of the legitimacy for the application of the Anti-Terrorism Law (Law No. 13.260/2016), as well as a case study of the first effective application of the Law. The new technological reality will be addressed through exploratory research aimed at analyzing a real possibility of cyber terrorist attack. The research method is bibliographic, through articles, criticism and reflections, pondering its impact on current criminal law. However, the possible destabilization of the State due to the spread of terror caused by this cybercrime cannot be ruled out, and an appropriate approach is necessary because of the degree of dangerousness, exceptionality and extent of damage based on the fundamental rights in our Constitution.

Keywords: Cyberterrorism; Internet; Deep web; Spread of Threat.

1 Introdução

No final da década de 60, a *Internet* estava sendo projetada pelos militares nos Estados Unidos da América com a finalidade de manterem sua superioridade tecnológica durante a Guerra Fria. Entretanto, com o acesso expandido pela sociedade, tal avanço tecnológico acarretou mudanças na nossa cultura. No Brasil, esse invento chegou apenas por volta de 1988, revolucionando os meios de comunicação, bem como dinamizando as formas de atuação de setores públicos e privados, tornando a sociedade moderna submissa a esse âmbito digital. É indiscutível que a *Internet* trouxe a proximidade da sociedade, reduzindo o tempo e o espaço. Nessa esteira, a *Internet* também trouxe contrariedades quanto a censura e liberdade na relação entre cidadão e Estado, seja ele nacional ou internacional.

Ademais, apesar dos benefícios proporcionados, o ciberespaço carrega questões contrárias quanto ao convívio em sociedade, no tocante ao estímulo de propagação de ideologias, bem como o terror fomentado na grande *World Wide Web,* precipuamente dentro da *Deep* e *Dark Web*[39]. As vulnerabilidades que esse âmbito carrega, tornou possível a

[39] A *Deep Web* e a *Dark Web* são níveis da World Wide Web (www) que representam a dobra invisível no ciberespaço, constituindo-se por todas as páginas que não foram – ou não puderam ser – indexadas pelos motores de busca.

existência de diversos tipos de condutas danosas e, por esse motivo, termos como ciberguerra, ciberataque e ciberterrorismo tomaram espaço no ordenamento jurídico de vários Estados do globo. Desse modo, o termo "ciberterrorismo" foi empregado pela primeira vez no ano de 1980 em um artigo redigido por Barry Collin (ALCÂNTARA, 2015), significando a junção do ciberespaço e do terrorismo convencional, para ataques conduzidos à longa distância, tornando a população refém do medo e ameaçando um Estado Democrático de Direito. Os danos causados por ciberterroristas no tocante à segurança do Estado advém da progressiva interdependência da sociedade moderna para com a tecnologia. 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 ciberterroristas se impõem.

Deste modo, apresenta-se uma adversidade em relação de como deve o ordenamento jurídico brasileiro ser aplicado diante um ataque desse porte. Tendo em vista as probabilidades de ocorrência do ciberterrorismo em esfera global, o presente estudo tem por escopo analisar as divergências entre essa modalidade de cibercriminalidade e terrorismo comum e de como deve o ordenamento pátrio abordar referido ato. Portanto, será feita uma análise acerca da legitimidade presente na Lei nº 13.260, de 16 de março de 2016 (Lei Antiterrorismo) para a adequada aplicação ao ciberterrorismo, assim como de demais normas esparsas presentes no ordenamento jurídico pátrio. Ademais, cumpre destacar que a referida Lei sofre críticas devido seu caráter de excepcionalidade perante o Código Penal vigente, confrontando princípios constitucionais, ainda que em tese tente os resguardá-los, como é o caso do art. 1, inciso I, da Lei Superior.

Desse modo, a presente pesquisa foi desenvolvida seguindo o método de revisão bibliográfica, justificando-se que se partiu de uma concepção abrangente de diversos autores para compreender o ciberterrorismo e sua forma de atuação, bem como seus impactos frente ao Estado e aplicação do Direito. Especificamente, o propósito desse estudo é conceituar os atos ciberterroristas, bem como verificar a aplicabilidade do regime para os casos a serem apresentados; identificar as características diferenciadoras de terrorismo comum e ciberterrorismo, seus objetivos e juntamente examinar o ciberespaço e suas dobras semióticas, relativamente à facilitação do ciberataque; explorar a legislação atual no tocante ao terrorismo, bem como propor uma melhor aplicação das normas ao referido cibercrime.

2 O tratamento legislativo do ciberterrorismo

2.1 Considerações acerca do Direito Penal do Inimigo

A polêmica quanto a necessidade de um Direito Penal de exceção se deu por Jakobs, na Alemanha, na década de 1980 com a teoria do denominado Direito Penal do Inimigo. Após alguns anos, em virtude da recusa das suas teses iniciais, o doutrinador voltou ao seu estudo flexibilizando-as e somente no ano de 2003 é que publicou sua teoria com o lançamento de um livro, tendo em vista os acontecimentos em 11 de Setembro de 2001. Conforme destaca Masson (2015, p. 107), a teoria de Jakobs "coloca em discussão a real efetividade do Direito Penal existente, pugnando pela flexibilização ou mesmo supressão de diversas garantias materiais e processuais até então reputadas em uníssono como absolutas e intocáveis". Ainda, Greco (2005, p. 214) explica sobre Direito Penal do Inimigo que:

> […] na perspectiva de JAKOBS, o direito penal pode ver no autor um cidadão isto é alguém que dispõe de uma esfera privada livre do direito penal, na qual o direito só está autorizado a intervir quando o comportamento do autor representar uma perturbação exterior; ou pode o direito penal atender ao autor como um inimigo, isto é, uma fonte de perigo para os bens a serem protegidos alguém que não dispõe de qualquer esfera privada, mas que pode ser responsabilizado até mesmo pelos seus mais íntimos pensamentos. O direito penal do inimigo otimiza a proteção dos bens jurídicos, o direito penal do cidadão otimiza esferas de liberdade […].

Portanto, diferente do Direito Penal comum, essa teoria propõe um modo desigual de tratamento para determinadas situações consideradas de emergência, devendo funcionar dentro do Direito. Assim, considera-se que tal sistema é fruto do medo e insegurança, permitindo uma aplicação imediata do poder punitivo estatal. Para Jakobs (1985, p. 753 *apud* GRECO, 2005) é possível "caracterizar o Direito Penal segundo a imagem do autor da qual ele parte", assim, considera-se que o Direito Penal do Inimigo é um Direito Penal do autor, por meio do qual é estereotipado que determinados indivíduos ou grupos de pessoas são inimigos, não importando o fato cometido. No pensamento do doutrinador, inimigo é a antítese do cidadão, ou seja, aquele indivíduo que não respeita e não reconhece as regras do Estado, pois se colocam acima deste. Nas palavras de Masson (2015, p. 107), inimigo para Jakobs é o indivíduo que:

> Afronta a estrutura do Estado, pretendendo desestabilizar a ordem nele reinante ou, quiçá, destruí-lo. É a pessoa que revela um modo de vida contrário às normas jurídicas, não aceitando as regras impostas pelo Direito

> para a manutenção da coletividade. Agindo assim, demonstra não ser um cidadão e, por consequência, todas as garantias inerentes às pessoas de bem não podem ser a ele aplicadas.

Desta feita, entende o autor da teoria que inimigo é um grupo restrito, ou seja, nem todo criminoso é considerado inimigo, sendo que a maioria deve ser tratada como cidadãos. Como exemplos de indivíduos considerados inimigos perante a teoria traçada por Jakobs, são os terroristas, integrantes de organizações criminosas, agentes de crimes contra a liberdade sexual e, de modo residual, os autores de infrações penais graves e perigosas (MASSON, 2015, p. 107). O principal meio de prova é a confissão, sendo possível que o Estado utilize da tortura para obtê-la, bem como para dissipar atos ilícitos do criminoso e seus cúmplices, tendo por base o princípio da proporcionalidade. Nessa perspectiva, coexistem dois direitos penais: Direito Penal do Cidadão, o qual é garantista, pois reconhece e respeita os direitos e garantias do ser humano previstos na Constituição Federal e nas Leis, típico de um Estado Democrático de Direito, bem como retrospectivo, porque tem como fundamento a culpabilidade; e o Direito Penal do Inimigo, o qual é autoritário, uma vez que suprime direitos e garantias do ser humano, e, ainda, é prospectivo, pois se baseia na periculosidade, ou seja, o inimigo é punido por aquilo que pode cometer futuramente. Nesse sentido, Masson (2015, p. 107) explica os efeitos da aplicação da teoria do Direito Penal do Inimigo:

> Inicialmente, o Estado não deve reconhecer os direitos do inimigo, por ele não se enquadrar no conceito de cidadão. Consequentemente, não pode ser tratado como pessoa, pois entendimento diverso colocaria em risco o direito à segurança da comunidade. O inimigo, assim, não pode gozar de direitos processuais, como o da ampla defesa e o de constituir defensor, haja vista que, sendo uma ameaça à ordem pública, desconsidera-se sua posição de sujeito na relação jurídico-processual. Possível, inclusive, a sua incomunicabilidade. [...].

Ainda, o Direito Penal do Inimigo deve antecipar a tutela penal para alcançar os atos preparatórios. Nesse sentido, o inimigo que praticar qualquer ato preparatório, é passível de punição, diferente do que ocorre no Direito Penal do Cidadão, em que apenas são passíveis de punição o primeiro ato executório para consumação do delito. Nesse aspecto da punição dos atos preparatórios, Asúa (1997, p. 472 *apud* ANDRADE, 2019) afirma que "na prática, a divisão entre os atos preparatórios e os atos executórios não é nada fácil. Ainda, a penalização dos atos preparatórios só faria sentido se o mesmo apresentar um perigo relevante, isto é, estiver próximo do cometimento do ilícito". Esse é o entendimento quanto ao atentado de 11 de setembro de 2001, em que vidas inocentes poderiam ter sido salvas caso a atuação de terroristas tivesse sido interrompida previamente (MASSON, 2015, p. 107). Nesse contexto,

tem-se que tal sistema adota a natureza de um Direito Penal de terceira velocidade, termo adotado por Jesus Maria Silva Sanchéz, pois indica um modelo criminal célere, possuindo um grau punitivo elevado, com a privação da liberdade e relativização ou eliminação de direitos e garantias penais e processuais. Esse cenário também abarca a ramificação do terrorismo convencional, qual seja, o ciberterrorismo. Coerente se faz o entendimento de que ambos delitos merecem um tratamento típico de um direito penal de emergência, afinal, possuem o intuito de atemorizar Estados e sociedades por motivos políticos, religiosos ou ideológicos.

Assim, constata Tangerino (2016):

> 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.

Nesse sentido, o Estado seria capaz de atuar no mesmo âmbito que os ciberterroristas, podendo aumentar as probabilidades de efetiva prevenção e punição da conduta ilícita praticada no ciberespaço por esse determinado grupo de indivíduos. Entretanto, se a atuação dos ciberterroristas forem além das linhas territoriais do respectivo Estado, certamente se gerará uma dificuldade na aplicação de sua soberania, pois se invocada, poderá ser em detrimento de outro Estado. Por tal razão, além da tipificação (que neste artigo será tratada), necessário a utilização de mecanismos que visem a prevenção/cooperação, que poderão ser observados a seguir.

2.2 O ciberterrorismo no Direito comparado

Como já explanado anteriormente, dada a complexidade de conceituação do terrorismo, este compreende uma difícil tipificação. A *World Wide Web* possibilitou a união das pessoas espalhadas pelo globo e, dessa mesma vantagem, também se permitiu a partilha de informações, coordenar atividades, disseminar propagandas de um jeito mais veloz e "muitas das vezes com o intuito do recrutamento, coordenar ataques e ainda angariar fundos" (MELO, 2017).

Assim, os sistemas jurídicos europeus e dos Estados Unidos da América, sofreram divergência quanto ao tratamento adequado para ataques terroristas. Enquanto ordenamentos jurídicos europeus tratavam referido crime do mesmo modo que qualquer outro, bem como o tratamento dos agentes do crime não recebeu tratamento mais gravoso quanto aos efeitos,

garantindo direitos materiais e processuais ao sujeito, nos EUA aplicou-se ao ordenamento o Direito Penal do Inimigo, suprimindo liberdades e garantias dos cidadãos. Diante os ataques sofridos, os EUA adotaram uma postura mais agressiva no tocante ao terrorismo e suas ramificações, que nos dizeres de Fasani (2016, p. 111-112 *apud* MELO, 2017) para eles tal ato é "[...] uma versão de crime superior e mais perigosa, uma espécie de super-crime que incorpora características de guerra". Neste entendimento, todos os indivíduos que sejam suspeitos de realizar qualquer conduta que preencha os requisitos do terrorismo, previstos em norma, seriam apresentados a uma Comissão Militar – e não a um juiz, como qualquer outro cidadão – e não são ponderados a determinados procedimentos, como por exemplo:

> a) todos os membros da Comissão Militar são nomeados pelo Presidente dos EUA ou pelo Secretário da defesa; b) o procurador-geral, o procurador e os seus assistentes são todos nomeados pelo Ministério da Defesa; c) todos os membros da *review panel* dependem do Ministério da Justiça; d) o arguido não toma necessariamente consciência de toda a prova a produzir contra si nem tampouco a identidade de eventuais testemunhas; e) o processo não é público; f) a Comissão pode ter em conta todos os elementos de prova, independentemente da sua fonte e da forma de ingresso no processo; g) o arguido não tem direito ao apelo a um juiz independente e *last but not least* para o condenado a pena pode surgir incerta e substancialmente discricionária por parte da Comissão que pode entre outras penas aplicar a própria pena de morte (MELO, 2017).

É desse modo, perante tais medidas adotadas, que se entende a aplicação do Direito Penal do Inimigo pelo ordenamento jurídico americano, tendo em vista que referidas medidas são consequências práticas do que a teoria de Jakobs pressupõe, como visto em tópico próprio. Ainda, diante a dimensão e gravidade do tema, imprescindível se torna analisar as precauções que os governos estrangeiros estão implementando na tutela do Estado contra ciberterrorismos. Desta feita, conforme já exposto, os EUA fortaleceram suas medidas contra o terror após o atentado ao *World Trade Center*, publicando o *USA Patriot Act* (THE UNITED STATES DEPARTMENT OF JUSTICE), o qual adota princípios legais já existentes e os adaptam para salvaguardar a vida e liberdade dos americanos diante outros possíveis ataques terroristas. À vista disto, o texto legislativo para tipificação do crime de terrorismo previu um rol de condutas, como por exemplo:

> Destruição de aeronaves; uso de armas nucleares, químicas ou biológicas; uso de armas de destruição em massa; bombardeio de propriedades do governo; sabotagem de instalações nucleares; pirataria de aeronaves; ataques terroristas a sistemas de transporte de massa; e ataque bioterrorista (THE UNITED STATES DEPARTMENT OF JUSTICE).

Além de tipificar condutas, o *USA Patriot Act* aumentou a pena máxima de crimes considerados passíveis de serem cometidos por terroristas, bem como aprimorou punições por conspiração, tais como "incêndio criminoso, destruição de instalações de energia, apoio material a terroristas e organizações terroristas e destruição de materiais de defesa nacional, assassinatos em instalações federais, ataques a sistemas de comunicações" (THE UNITED STATES DEPARTMENT OF JUSTICE). Neste mesmo Estado foram criados departamentos para desenvolver planos nacionais visando a proteção da infraestrutura do governo. Nesse sentido, Medero (2012, p. 252 *apud* COSTA, 2017) aduz em sua pesquisa que "[...] o "*Critical Infrastructure Assurance Office*" (CIAO) e o *National Infrastructure Protection Center* (NIPC) foram criados para salvaguardar ataques cibernéticos contra redes de infra-estrutura (*sic)* e sistemas nacionais". Destarte, a lei americana além de tipificar condutas terroristas, também previu condutas ciberterroristas, adotando medidas de vigilância como por exemplo:

> O uso de novas tecnologias para fins investigatórios; a utilização de ferramentas já disponíveis para a investigação do crime organizado e de tráfico de drogas, como a interceptação telefônica; a emissão de mandados de busca contra suspeitos de terrorismo no intuito de evitar fuga, destruição de provas, intimidação ou homicídio de testemunhas; o acesso, mediante autorização judicial, a dados bancários para verificar quem está enviando dinheiro para terroristas; o acesso, também precedido de autorização judicial, a registros de vendas de lojas para apurar quem comprou materiais para fabricação de explosivos; a facilitação de compartilhamento de informações e cooperação entre agências do governo; e, ainda, o auxílio a vítimas no combate a *hackers* (ALMEIDA et. al, 2017).

Desta feita, devido a pontualidade e o rico tratamento dado ao fenômeno pelo governo americano, demais países o utilizam como embasamento para tratar o mesmo tema. Nesse sentido, enfatiza Menezes (2012, p. 22 *apud* COSTA, 2017):

> A lei americana de combate ao terrorismo funciona como modelo para definir um padrão mundial de segurança. Mediante rastreamento é possível identificar e punir, de acordo com as leis internacionais, quem promover algum tipo de vandalismo eletrônico. O rastreamento é medida adotada também pela maioria dos países europeus, adotando o padrão americano, nas suas estratégias de combate ao ciberterrorismo.

Não obstante os Estados Unidos serem o país que se encontra à frente quanto ao aprimoramento de seu ordenamento jurídico no tocante ao ciberterrorismo, o Reino Unido também possui normas rígidas com o intuito de obstar e punir condutas ciberterroristas, visto que o legislador britânico promulgou o denominado *Terrorism Act 2000,* a primeira legislação antiterrorista no Reino Unido. Tempos mais tarde, em 11 de abril de 2006, expediu o

Terrorism Act 2006 e, dois anos depois, o *Terrorism Act 2008*, o qual prevalece até os dias de hoje e apenas incrementou os poderes da polícia no tocante aos delitos já previstos nas duas legislações anteriores. O site *Legislation.Gov.Uk* utilizou a definição de terrorismo contido na lei anterior, porém incluiu tipos específicos[40]. Na seção 1(1)(b) definiu tal conduta como sendo "quando o uso ou ameaça é projetada para influenciar o governo ou uma organização governamental internacional ou intimidar o público ou uma parte do público", e na seção 1(1)(c) quando "o uso ou ameaça é feito com o objetivo de promover uma causa política, religiosa, racial ou ideológica.". Ainda, o *Legislation.Gov.Uk* já previa a criminalização do ciberterrorismo na seção 1(2)(e) enquadrando a ação quando for "projetada seriamente para interferir ou interromper seriamente um sistema eletrônico". Portanto, resta evidente que os governos estrangeiros já estão em alerta quanto a essa novidade de cibercriminalidade, inovando seus ordenamentos jurídicos com o intuito de efetivar medidas quanto a um possível ataque ciberterrorista.

2.3 Ordenamento jurídico brasileiro no combate ao ciberterrorismo

Após verificar a legislação estrangeira no tocante ao ciberterrorismo, importante analisar como o Brasil vem tratando o tema em leis esparsas, bem como desde a promulgação da Constituição Federal em 1988. Destaca-se que 5 (cinco) anos antes foi promulgada a Lei de Segurança Nacional (Lei nº 7.170/83), prevendo os crimes que lesam ou expõem a perigo de lesão à ordem política e social, bem como a segurança nacional. Ainda, trouxe, em seu artigo 20, uma tentativa de definição do terrorismo. Entretanto, o objetivo não foi atingido, uma vez que referido artigo limitou-se à expressão "atos de terrorismo". Imperioso mencionar que, referido artigo foi alvo de críticas devido a "impressão e vagueza, sendo denominada uma violação ao princípio da taxatividade (*lex certa*), corolário do princípio da legalidade" (ALMEIDA *et. al*, 2017, p. 145). Passados cinco anos da publicação da Lei de Segurança Nacional, foi promulgada a vigente Constituição Federal, trazendo artigos que tratam do terrorismo. O artigo 1º, inciso I da nossa Carta Magna traz em seu bojo

> [...] um dos princípios fundamentais, autorizando-se a leitura de que, indiretamente, o país não tolerará forma de intervenção oficial ou clandestina, neste último caso podendo ser incluído o terrorismo. Em seguida, o legislador constituinte elegeu, como objetivo fundamental, nos incisos I e IV do artigo 3º, a construção de sociedade livre, justa e solidária, além do compromisso de promover o bem de todos, sem preconceitos de

[40] A informação aqui apresentada encontra-se disponível no referido site.

> origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação, o que justifica uma negação ao terrorismo praticado sob as bandeiras do fundamentalismo religioso (CALLEGARI; LIRA, 2015, p. 732 *apud* COSTA, 2017).

Ao não aceitar a intervenção oficial ou clandestina, o artigo 1º, inciso I da Constituição Federal demonstra a sua soberania. Através deste mecanismo, é garantido o poder de decidir em última instância sobre a eficácia do direito para sociedade nos limites territoriais brasileiro (DALLARI, 1998, p. 80). Deste modo, o ato terrorista praticado em solo brasileiro, por se tratar ato contra o Estado (ainda que atinja pessoas físicas e jurídicas) afeta diretamente o poder soberano brasileiro, o que ocasiona na aplicação jurídica que o ordenamento brasiliano, ainda que os agentes terroristas sejam de outras nações.

É com base na noção de soberania brasileira e de outros Estados-Nações, que o artigo 4º reconhece o repúdio ao terrorismo como um dos princípios básicos das relações internacionais. Já internamente, o artigo 5º, em seu inciso XLIII equiparou o terrorismo a crime hediondo, extinguindo a possibilidade de concessão da fiança, graça e anistia, e dos quais se punem "[...] os mandantes, os executores e os que, podendo evita-los, se omitirem". Ainda, os artigos 2º, 5º, inciso V, e 8º da Lei de Crimes Hediondos (Lei nº 8.072/1990) trazem o mesmo repúdio ao terrorismo. Outro dispositivo legal que aborda o tema é a Lei de Organização Criminosa (Lei nº 12.850/2013), elucidando em seu artigo 1º, §2º, inciso III, que os procedimentos investigatório e criminal, bem como infrações correlatas que nela se encontram, serão aplicadas às organizações criminosas e também: "às organizações terroristas, entendidas como aquelas voltadas para a prática dos atos de terrorismo legalmente definidos". Ainda, integrando a legislação pátria, o Brasil ratificou diversas convenções e protocolos internacionais que tratam acerca do terrorismo:

> De fato, o Brasil ratificou pelo menos 15 convenções e protocolos internacionais de combate ao terrorismo. São eles: Convenção Relativas às Infrações e Certos Outros Atos Cometidos a Bordo de Aeronaves; Convenção para Repressão ao Apoderamento Ilícito de Aeronaves; Convenção para Prevenir e Punir os Atos de Terrorismo Configurados em Delitos contra as Pessoas e a Extorsão Conexa Quando Tiverem Eles Transcendência Internacional; Convenção para a Repressão de Atos Ilícitos contra a Segurança da Aviação Civil; Convenção sobre a Prevenção e Punição de Infrações contra Pessoas que Gozam de Proteção Internacional, incluindo os Agentes Diplomáticos; Convenção contra a Tomada de Reféns; Convenção sobre a Proteção Física dos Materiais Nucleares; Protocolo para a Supressão de Atos Ilícitos de Violência nos Aeroportos a Serviço da Aviação Civil; Convenção sobre a Marcação dos Explosivos Plásticos para Fins de Detecção; Convenção Interamericana Contra a Fabricação e o Tráfico Ilícito de Armas de Fogo, Munições, Explosivos e Outros Materiais Correlatos; Convenção Internacional sobre a Supressão de Atentados

> Terroristas com Bombas (com reserva ao parágrafo 1 do artigo 20); Convenção Internacional para a Supressão do Financiamento do Terrorismo; Convenção Interamericana Contra o Terrorismo; Convenção para a Supressão de Atos Ilícitos contra a Segurança da Navegação Marítima; Protocolo para a Supressão de Atos Ilícitos contra a Segurança de Plataformas Fixas localizadas na Plataforma Continental. Ademais, o Brasil assinou, em 13 de abril de 2005, a Convenção Internacional para a Supressão de Atos de Terrorismo Nuclear, mas ainda não a ratificou (LASMAR, 2015, p. 58).

A última Convenção de que Lasmar se refere – Convenção Internacional para a Supressão de Atos de Terrorismo Nuclear – foi ratificada e promulgada pelo Decreto nº 9.967, de 08 de agosto de 2019. Destarte, apesar de todo o material legislativo demonstrado, o terrorismo ainda era indefinido, pois não dispunha de um tipo penal próprio e muito menos uma definição jurídico-penal apropriada. Conforme aponta Lasmar, as características do terrorismo revelam adversidades ao nosso sistema penal vigente:

> Afinal de contas, os sistemas criminais são desenhados para responder e punir crimes após seu acontecimento, mas o objetivo primário de estratégias, políticas e legislações de combate ao terrorismo devem ser exatamente evitar ou prevenir os incidentes. Por isso, muitos dos mecanismos e procedimentos penais existentes são ineficazes ou inadequados para responder a esse fenômeno e daí a necessidade de se criar uma legislação sistemática específica (LASMAR, 2014, p. 68 *apud* COSTA, 2017).

Toda essa trajetória legislativa traçada pelo Brasil, na tentativa de tipificar e punir o terrorismo, ainda integrava a conduta ciberterrorista. Nesse aspecto, o legislador não havia se preocupado com referida questão, visto que se tornou um problema anos após a expansão da *Internet* no âmbito nacional. A observação trazida por Lasmar no tocante as adversidades entre as características do terrorismo e o sistema penal vigente, é também aplicável ao ciberterrorismo, pois, conforme visto, atua no ciberespaço possuindo um *modus operandi* divergente do terrorismo convencional. Assim, devido a desterritorialização, uma operação ciberterrorista é passível de "causar uma grande reação, nas relações interconectadas pelo mundo virtual da sociedade contemporânea internacional" (BARROS, 2015, p. 41 *apud* COSTA, 2017).

Portanto, além da tipificação da conduta do ciberterrorismo, fez-se necessário a elaboração de um sistema penal que, além de punir tais condutas, operasse no prisma da prevenção, com meios investigativos e específicos nesse âmbito, objetivando a proteção do Estado como um todo. Assim sendo, em 2016 foi promulgada a Lei Antiterrorismo (Lei nº 13.260/2016), apresentando um avanço no ordenamento jurídico Brasileiro no tocante ao ciberterrorismo. Entretanto, ainda pairam críticas da referida Lei, pois esta mostra-se

insuficiente quanto ao tema, não tendo o abordado adequadamente e com propriedade, conforme será demonstrado em subtópico específico.

3 Mandados de criminalização na Constituição Federal de 1988 no âmbito do terrorismo

Antes de adentrar aos comentários acerca da Lei Antiterrorismo, necessário se faz a compreensão do motivo que fez surgir tal Lei. Conforme visto, a CF em seus artigos 4º e 5º repudiam a prática terrorista. Dentro do artigo 5º, especificamente no inciso XLIII, faz menção a uma Lei própria para referido crime. Assim, a teoria dos mandados de criminalização surgiu no Brasil com a decisão do Recurso Extraordinário nº 418.376-5/MS. Referida decisão sustentava que a doutrina vinha apresentando a existência de uma espécie de garantismo positivo, de modo que proibição de proteção limitada era de grande importância na aplicação dos direitos fundamentais de proteção, notadamente nos casos em que "o Estado não pode abrir mão da proteção do direito penal para garantir a proteção de um direito fundamental." (SUPREMO TRIBUNAL FEDERAL, 2006). Portanto, a teoria dos mandados de criminalização constitui-se em um instrumento da Constituição Federal, tendo por objetivo viabilizar a proteção suficiente e justa de direitos fundamentais, cada vez que se encontrem lesionados ou ameaçados por agentes públicos ou particulares. Conforme Antônio Carlos da Ponte (2008 *apud* PONTE, KAZMIERCZAK, 2017) tais mandados "indicam matérias sobre as quais o legislador ordinário não tem a faculdade, mas a obrigatoriedade de tratar, protegendo determinados bens ou interesses de forma adequada e, dentro do possível, integral". Nesse sentido, para acompanhar a evolução histórico-social, surgiu um novo modelo de proteção de direitos. Assim, o Estado, antes guardião dos direitos fundamentais do cidadão, agora tem como função precípua a proteção dos direitos fundamentais de dimensão individual e metaindividual. Nessa linha, Baratta (1999, p. 110 *apud* GAVIÃO, 2008) entende que:

> Esse novo modelo de Estado deverá dar a resposta para as necessidades de segurança de todos os direitos, inclusive de ordem prestacional (direitos sociais, econômicos e culturais), e não somente daqueles direitos chamados de prestação de proteção, em particular contra agressões de natureza delitiva praticada por determinadas pessoas.

Nessa acepção, o Supremo Tribunal Federal reconheceu a dupla face de garantias, tendo decidido no Habeas Corpus nº 104.410/RS que

> Os direitos fundamentais não podem ser considerados apenas como proibições de intervenção (*Eingriffsverbote*), expressando também um postulado de proteção (*Schutzgebote*). Pode-se dizer que os direitos fundamentais expressam não apenas uma proibição do excesso (*Übermassverbote*), como também podem ser traduzidos como proibições de proteção insuficiente ou imperativos de tutela (*Untermassverbote*) (ALMEIDA *et. al*, 2017, p. 175)

Portanto, a Constituição Federal Brasileira possui natureza tanto garantista quanto impositiva, pois traz em seu bojo a obrigatoriedade do legislador infraconstitucional tutelar interesses no âmbito do Direito Penal, estabelecendo um número de cláusulas que carecem de proteção. Assim, o legislador deve atuar salvaguardando direitos fundamentais e a própria soberania através do procedimento penal. Nos artigos 1º e 3º da Carta Magna, são elencados os fundamentos dos mandados de criminalização. De acordo com referidos artigos, é indispensável que os bens ou valores desprovidos de tutela, derivam dos fundamentos (art. 1º) ou dos objetivos fundamentais (art. 3º) da República Federativa do Brasil. Quanto a ordem da criminalização, poderá ser feita de forma expressa ou implícita. Contudo, perante o foco do presente trabalho, deve-se atentar apenas quanto a primeira espécie. Ao perfazer uma análise da Constituição Federal, Ponte cita exemplos de mandados expressos de criminalização:

> artigo 5º, incisos XLII (racismo), XLIII (tortura, tráfico ilícito de entorpecentes e drogas afins, terrorismo e crimes hediondos) e XLIV (ação de grupos armados, civis ou militares, contra a ordem constitucional e o Estado democrático), e §3º (os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais); artigo 7º, inciso X (retenção dolosa do salário dos trabalhadores); artigo 225, § 3º (condutas lesivas ao meio ambiente); e artigo 227, §4º (abuso, violência e a exploração sexual da criança ou adolescente) (PONTE, 2008 *apud* PONTE, KAZMIERCZAK, 2017).

Imperioso observar que a Carta Magna possui um vasto rol de mandados de criminalização – tanto expressos quanto implícitos. Mais uma vez, diante ao objetivo precípuo desta pesquisa, a análise dos mandados de criminalização será restringida àquela prevista no artigo 5º, inciso XLIII, pela qual é determinado o dever de criminalizar o terrorismo, que foi cumprido por meio da Lei nº 13.260, de 16 de março de 2016, conhecida como Lei Antiterrorismo.

3.1 Comentários à Lei Antiterrorismo (13.260/2016) sob o prisma do ciberterrorismo

No ano de 2016 ocorreu o evento das Olímpiadas no Brasil, realizada no Rio de Janeiro, e, diante disso, para nivelar-se com a política criminal antiterrorismo dos países estrangeiros, no mesmo ano foi promulgada a Lei nº 13.260, regulamentando o disposto no inciso XLIII do artigo 5º da Constituição Federal, de modo a tipificar atos terroristas. A motivação da criação da referida lei foi a possibilidade de um atentado ser realizado durante o evento, prevendo a lei pena de "reclusão de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência". Além disso, a lei especial em comento trata acerca de crimes relacionados ao terrorismo nos artigos 3º a 6º, bem como das disposições investigatórias e processuais. Em seu artigo 2º, é trazido o conceito de terrorismo:

> […] 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.

Fazendo uma análise do dispositivo acima transcrito, Almeida realiza uma interpretação gramatical e restritiva de que, na Lei em comento, o crime de terrorismo é o único equiparado a hediondo, pois possui previsão no artigo 2º, sendo que os demais delitos previstos não tipificam o terrorismo, mas somente a ele se comparam:

> Nesta relação, é mantida a autonomia de cada tipo penal, mas que encontra na vigência e validade do art. 2º um pressuposto abstrato para sua aplicação, por exemplo: para que reste caracterizado o crime de integrar uma organização terrorista, exige-se que esta esteja voltada para a prática do art. 2º, §1º (art. 3º c/c art. 19); para que seja configurado o delito de fornecer ou receber treinamento em país distinto daquele de sua residência ou nacionalidade, deve o agente ter o propósito de praticar algum dos atos do art. 2º, §1º (art. 5º, §1º, II); para que se incorra no crime do art. 6º, a conduta precisa estar voltada para o planejamento, a preparação ou execução dos crimes previstos nesta Lei, o que significa estar voltada para o art. 2º ou aos demais delitos que, por seu turno, têm no art. 2º um pressuposto abstrato (ALMEIDA *et al.* 2017, p. 163).

Portanto, os crimes previstos nos artigos 3º a 6º são delitos autônomos que, segundo a Almeida (*et al.* 2017, p. 163)., se por ventura o artigo 2º tornar-se inválido, são passíveis de se tornarem inaplicáveis devido a inexistência de pressuposto abstrato. Por outro lado, há uma segunda corrente doutrinária defendida pelos Mestres Rogério Sanches Cunha e Ronaldo Batista Pinto de que todos os tipos penais previstos nesta Lei são crime de terrorismo, logo, são comparados a hediondo. Segundo os autores, a Lei 13.260/2016 regulamenta o disposto no artigo 5º, inciso XLIII da CRFB/88, caracterizando como uma "verdadeira lei de regência e como tal cria um sistema de prevenção e repressão ao terrorismo (antiterror)" (ALMEIDA

et al. 2017, p. 163). Tal entendimento dos exímios autores tem por base o princípio da proteção deficiente:

> Todos os crimes da Lei 13.260/2016 são equiparados a hediondo. Da mesma forma que não se deseja uma hipertrofia da punição, deve-se buscar evitar a proteção deficiente do Estado na tutela dos bens jurídicos indispensáveis à convivência do homem em sociedade, especialmente no caso de crimes como os aqui tipificados, de massa, com vítimas indefinidas ou indeterminadas (ALMEIDA *et al.* 2017, p. 173).

Assim, Rodrigo Carneiro Gomes (2016) retrata que a definição legislativa do terrorismo é estruturada da seguinte maneira:

> a) Número de agentes: É desnecessária a pluralidade de agentes. Basta a prática de atos descritos como de terrorismo (artigo 2º, parágrafo 1º) por qualquer pessoa (um ou mais indivíduos), sendo crime comum, unissubjetivo; b) Motivação do agente: Atua por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião. Não foram incluídas a motivação política e a supressão de valores democráticos, no que a legislação poderia ser mais avançada; c) Elemento subjetivo: Atuação com o fim especial de provocar terror social ou generalizado, com exposição a perigo de pessoa, patrimônio, da paz pública ou da incolumidade pública. Basta a verificação do estado anímico ou da psique do agente, sendo desnecessário perquirir se, efetivamente, foi provocado terror, mas a consubstanciação da exposição a perigo é essencial do tipo; d) Meio: Explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares, mecanismos cibernéticos, sabotagem, violência, grave ameaça, atentados; e) Elemento objetivo: Praticar atos de terrorismo previstos no artigo 2º, parágrafo 1º.

No presente trabalho, relevante é a análise no que tange o parágrafo primeiro, inciso IV do artigo 2º, o qual dispõe, *in verbis*:

> § 1º São atos de terrorismo: 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;

De acordo com os doutrinadores, tal dispositivo trata de tipo misto alternativo, de conteúdo variado ou de ação múltipla. Nesse aspecto, o agente que dolosamente praticar mais de um dos verbos nucleares previstos, dentro do mesmo contexto fático, responderá por um único crime, por força do princípio da alternatividade. Como pode-se observar, a legislação pátria cuida do ciberterrorismo como uma vertente do terrorismo, de modo que prevê condutas já penalmente tuteladas fora do

ciberespaço e as qualifica dentro desse âmbito. Ainda, ao utilizar as expressões, no *caput*, "por razões de" e "quando cometidos com a finalidade de", tem-se que o elemento subjetivo é o dolo, ou seja, o desejo consciente de efetivar a conduta descrita no tipo penal. Portanto, o legislador nacional finalmente tratou da conduta ciberterrorista no dispositivo *supra*, condicionando à observância do disposto no *caput* do mesmo artigo, ou seja, deverá dar-se 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.

No dispositivo mencionado, o bem jurídico tutelado pelo legislador foram os patrimônios e serviços públicos e privados, a incolumidade pública e a paz pública. Ainda, pode-se extrair que trata de crime comum, pois tais delitos podem ser praticados por qualquer indivíduo, seja só ou em colaboração com outrem. Nesse sentido, "o sujeito passivo imediato é o ente que detém o controle dos bens ou serviços enumerados neste inciso, bem como a coletividade. Já o sujeito passivo mediato é o Estado" (ALMEIDA *et al*., 2017, p. 209). O crime será consumado quando o agente sabotar o funcionamento ou apoderar-se, servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, do meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, 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. Por tratar-se de um crime formal, é prescindível o dano a algum desses objetos materiais pela sabotagem ou apoderamento de seu controle. Porém, imprescindível que a conduta exponha a perigo pessoa, a paz pública, a incolumidade pública ou o patrimônio que não o diretamente atingido pela conduta. A doutrina classifica tal norma como sendo um crime

> Pluriofensivo (ofende a mais de um bem jurídico), comum (não exige condição ou qualidade especial do sujeito ativo, podendo ser praticado por qualquer pessoa), unissubjetivo ou unilateral ou de concurso eventual (perpetrado por um só agente, admitindo colaboração de outrem), de dupla subjetividade passiva (há dois sujeitos passivos), de perigo comum (expõe a risco um número indeterminado de pessoas), de ação múltipla ou de conteúdo variado ou tipo misto alternativo (há mais de um verbo nuclear), formal ou de consumação antecipada ou de resultado cortado (a consumação se dá com a realização da conduta, sendo prescindível a ocorrência de resultado naturalístico), de forma vinculada (o tipo enumera os meios de execução), de perigo concreto (exige perícia para fins de comprovação do potencial lesivo), comissivo (cometido por meio de ação) e plurissubsistente (é possível o fracionamento do *iter criminis*, sendo cabível a tentativa) (ALMEIDA et al., 2017, p. 209).

Ainda sobre o artigo 2º, o tipo criminaliza condutas apenas quando praticadas em razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião. Diante dessa norma, passaremos a analisar um exemplo ocorrido em 2017: o ciberataque global, em que foi

utilizado um *vírus malware* denominado *WanaCrypt0r*, bloqueando o acesso a arquivos mediante uma codificação, com o prometimento de liberá-los apenas mediante pagamento.

Esse incidente acarretou consequências em vários países, como por exemplo, no Reino Unido, em que desestabilizou o Serviço Nacional de Saúde, paralisando o funcionamento dos computadores e telefones de pelo menos 16 hospitais, e ainda, eliminando temporariamente os respectivos sistemas (EL PAÍS, 2017). Na Alemanha o sistema de controle de rede ferroviária, movida pela *Internet*, também foi afetada. Já no Brasil, foram afetados os sistemas de processos eletrônicos do Tribunal de Justiça e do Ministério Público de São Paulo, os quais foram retirados do ar preventivamente, a Petrobrás e o Instituto Nacional do Seguro Social (INSS) suspenderam suas atividades como medida de segurança (EL PAÍS, 2017).

Diante tais informações, referido ciberataque não configuraria o crime de ciberterrorismo, tendo em vista que não fora praticado dentro dos motivos exigidos pela norma criminalizadora. Assim, a Lei nº 13.260/2016 não seria a ele aplicada mesmo que tenham os agentes sabotado por meio de mecanismos cibernéticos, ainda que de modo temporário, o funcionamento de alguns entes previstos no inciso IV do artigo em comento (meio de comunicação – telefone, estações ferroviárias, hospitais e locais onde funcionem serviços públicos).

Do mesmo modo, a promessa de liberação dos sistemas mediante pagamento evidencia que os agentes almejavam obter vantagem econômica, outro ponto que afasta o dolo do ciberterrorismo, uma vez que a norma não prevê tal finalidade. Neste condão, a lei brasileira ao condicionar atos de terrorismo a razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, reduz a proteção ao bem jurídico ao qual propõe-se a proteger, e, ainda, o agente é submetido a critérios subjetivos por parte do julgador.

Contudo, se as condutas acima pontuadas fossem acompanhadas de motivação preconceituosa ou xenofóbica certamente afetaria a soberania brasileira, já que seria uma intervenção clandestina na atuação estatal. A pior situação ocorreria se estas condutas fossem reiteradamente praticadas, já que surgirá a possibilidade de uma guerra cibernética, que resultaria em igual ou maior letalidade se comparada as guerras convencionais (BENELLI, 2018, p. 07). A criação da respectiva Lei demonstra que o Estado brasileiro além de resguardar o ciberespaço a ele inerente, pontua de forma legal uma tutela ao seu poder soberano e o faz com base no art. 1, inciso I, da Constituição Federal.

Sem postergar mais sobre o assunto, critica-se a amplitude do artigo 3º ao criminalizar as condutas de promover, constituir, integrar ou prestar auxílio, pessoalmente ou

por interposta pessoa, a organização terrorista, sem detalhar e delimitar os meios utilizados para a prática do primeiro verbo do tipo. Nesse sentido, será possível supor que "a promoção realizada por um integrante de um pequeno grupo de mensagens por meio de aplicativos para telemóveis, limitado a algumas dezenas de pessoas, pode ser meio de promoção e consequente punição pela legislação" (SOUZA, 2019). Tal crítica merece respaldo, pois a conduta "promover" pode ser realizada de diversas formas, tendo em vista que se encontra tipificada em um país que possui uma sociedade com acesso à *Internet* e tecnologias que facilitam a troca de informações instantaneamente. Dessa forma, torna-se incoerente tal amplitude dentro de uma legislação que tem por fim obstar e punir atos terroristas e suas ramificações.

Destarte, ao criar a Lei nº 13.260/2016, o legislador teve como objetivo defender o Estado e não seus cidadãos, indo de encontro com a teoria de Jakobs, uma vez que a lei, em seu âmago, torna o indivíduo criminoso por sua periculosidade e não pela conduta praticada. Nesse sentido, a Lei em seu artigo 5º antecipa a tutela penal ao criminalizar os atos preparatórios do *iter criminis* com a mesma pena do delito consumado, diminuída de um quarto até a metade. Contudo, já há discussões doutrinárias no entendimento de que referido artigo fere o princípio da presunção de inocência, tendo em vista a tentativa de criminalizar condutas que ainda não existiram ou que podem não ser criminosas posteriormente. Ainda, o artigo 5º contraria o Código Penal vigente, pois tipifica um crime já na forma consumada e não o objetivo de consumá-lo. Vide comentário sobre o que foi exposto:

> [...] ao tipificar "atos preparatórios de terrorismo", a lei passa admitir, somente em tese, que qualquer coisa possa vir a constituir ato preparatório para o terrorismo. Citam os autores os seguintes exemplos: (a) um sujeito decide viajar a um país conhecido por abrigar grupos extremistas; (b) estudantes que, por meio de fóruns de discussão na internet, discorrem sobre a "opressão do ocidente contra o oriente e, num certo dia, decidem reunir-se pessoalmente; (c) numa conversa interceptada, um dos interlocutores, de forma jocosa, diz que gostaria de "explodir" o Congresso Nacional (MARTINELLI; DE BEM, 2016, p.11 *apud* RODRIGUES, 2017).

Assim, entende-se que o legislador errou ao punir os atos preparatórios, uma vez que a própria lei incluiu alternativa de condutas previstas para a fase dos atos executórios, tais como a desistência e o arrependimento pelo agente, não tendo coerência em aplicá-los aos atos preparatórios. Ademais, o ordenamento jurídico brasileiro considera que o fato se defina após julgado, pois, ao contrário, vincularia o perigo a pessoa e não o perigo ao fato por ela praticado.

Portanto, o Direito Penal do Inimigo, consagrado por Jakobs e aplicado de modo implícito na Lei 13.260/2016, lesa a ordem constitucional do Estado brasileiro, uma vez que afronta princípios previstos na Carta Magna, tais como isonomia e presunção de inocência, não devendo haver um Direito Penal para cidadãos e outro excepcional para supostos inimigos – mister destacar que o Brasil possui o poder de decidir quais condutas penalizar, ainda que a ameaça seja a nível internacional e que outros países tenham optado pela imposição de medidas drásticas, como é o caso do EUA – .Desse modo, compreensível o entendimento de que a legislação carece de reforma, bem como de maior debate com a doutrina penalista.

4 A efetiva aplicação da Lei Antiterrorismo: Operação *Hashtag*

A denominada Operação *Hashtag,* deflagrada pela Polícia Federal (PF), foi a primeira a ter embasamento na Lei Antiterrorismo. Em julho de 2016, às vésperas dos Jogos Olímpicos sediado no Brasil, a Operação deteve um total de quatorze suspeitos de preparação de ato terrorista em prisão temporária. A investigação foi presidida pela Divisão Antiterrorismo da Polícia Federal (DAT), por meio da qual foi revelado a existência de um grupo de indivíduos formado por brasileiros, que, supostamente, pretendiam um ataque terrorista durante o evento que ocorreria na capital do Rio de Janeiro.

Segundo as investigações, o grupo se proclamava como "Defensores da Sharia" (RODRIGUES, 2017) e se comunicavam através dos aplicativos *WhatsApp* e *Telegram,* tendo sido considerados pela Polícia Federal como uma organização terrorista, e, por este motivo, os autores foram enquadrados no artigo 3º da Lei nº 13.260/2016 por promover a organização terrorista, instigação de outros indivíduos e propagação de ideias visando provocar terror generalizado e atentar contra vida ou integridade física de terceiros.

O delegado federal ao analisar no teor das conversas a possibilidade de os suspeitos estarem em posse de explosivos e armas de fogo, requereu a prisão preventiva dos suspeitos envolvidos em maior participação com o grupo e, para os de menor participação, a condução coercitiva e prisão temporária. Ainda, conforme consta na investigação, os suspeitos dialogavam sobre possíveis alvos durante os Jogos, tais como, estrangeiros, homossexuais, muçulmanos xiitas e judeus. Nos termos da acusação do Ministério Público Federal, o grupo se dedicava a "criar uma célula do Estado Islâmico no país" (ALESSI, 2017).

Em manifestação, o MPF foi favorável aos pedidos do delegado responsável pela investigação com relação a busca e apreensão domiciliar, condução coercitiva e prisão

temporária. No transcorrer do processo, a Defensoria Pública da União pediu a nulidade da denúncia, tendo em vista que os detidos na Operação não foram assistidos por advogados durante os interrogatórios iniciais, configurando, nesse caso, o cerceamento de defesa e colheita irregular de provas (ALESSI, 2017). Além disso, a defesa ainda alegou que:

> Nenhum dos acusados adquiriu artefatos terroristas, traçou planos de atentado, adquiriu passagens rodoviárias ou aéreas, ou detinham documentos com efetivo intento migratório e de engajamento terrorista, além de estarem geograficamente distantes. Outro argumento dos advogados é que parte das provas teriam sido colhidas de forma irregular nos grupos de conversa do Telegram, por um "agente infiltrado não-policial" e "sem autorização judicial" (ALESSI, 2017).

Diante todas as alegações e pedidos postulados, o juiz indeferiu-os e prolatou a sentença, condenando 8 dentre os 14 suspeitos, com fundamento na Lei Antiterrorismo, enquadrando os acusados nas leis: artigo 3º e 5º da Lei nº 13.260/2016 por integração de organização terrorista e ato preparatório de terrorismo; Lei nº 12.850/2013 por indício de ocorrência de crimes de organização criminosa; Lei nº 7.716/89 por racismo; Lei nº 7.170/83, por propaganda de perseguição religiosa; Lei nº 2.889/56 por genocídio; e na Lei nº 8.069/90, por corrupção de menor, visto que foi constatado um membro do grupo com idade inferior a 18 anos (CURITIBA, 2017).

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.

Necessário frisar que a situação apresentada neste capítulo ainda que não tenha sido acompanhada por outros ataques, pode fomentar uma realidade da qual não a sociedade brasileira não é habituada, principalmente no ciberespaço. Em função disto, serviços públicos poderão ser afetados (vide citação sobre o ataque ao Tribunal de Justiça de São Paulo, ainda que não considerada como ato ciberterrorista) se a atuação estatal for falha. Os resultados da Operação *Hashtag* ainda que exitosos, podem ser apenas um prelúdio do que pode acontecer.

O que se pode observar é que através de sanções judiciais, o Estado Brasileiro adotou medidas que podem serem consideradas como "ciberdefesa", que consistem na "monitorização, prevenção e resposta às ameaças que ponham em risco a soberania e segurança nacional" (RALO, 2013, *apud* CARVALHO, 2019, p. 231). Mediante tal aplicação, possibilita-se a proteção da soberania e da sociedade a ela pertencente seja no

espaço material ou virtual, sem em qualquer momento desrespeitar a Lei Superior que nos orienta.

5 Considerações finais

É inegável que a *Internet* foi uma das melhores ferramentas tecnológicas criadas, tendo em vista como facilitou a vida humana, de forma que o ciberespaço trouxesse uma nova e aprimorada forma de vivência em sociedade. Com tamanha amplitude desse ambiente digital, além de benefícios trouxe também desvantagens, como a criação de diversos crimes e o ciberterrorismo.

O ciberterrorismo é uma vertente do terrorismo convencional que se desenrola no ciberespaço, tendo as mesmas finalidades: ameaçar e intimidar governos ou sociedades, por meio do pânico e do medo, para atingir seus objetivos, seja por razões políticas, religiosas, racistas. Desse modo, o ciberterrorismo potencializa o crime de terrorismo comum, posto que se desdobra no ciberespaço, um ambiente virtual de comunicação e transmissão de dados através da interconexão global dos computadores ou qualquer outro aparelho tecnológico. Ademais, o ciberespaço não comporta fronteiras, tendo como principal característica a velocidade em que os atos circulam, diferentemente do mundo físico. A porta de entrada para o ciberespaço é a *Internet*, sendo melhor interpretada devido a *World Wide Web*, um sistema documentos em hipermídia interligados, compreendendo dobras semióticas que se subdivide em três níveis: *Surface Web*, *Deep Web* e *Dark Web*. Dessa forma, o ambiente cibernético constitui uma verdadeira complexidade, com sistemas de interação intricados e abertos, sendo que uma ação é capaz de gerar uma grande reação. Ademais, o ciberespaço possui vulnerabilidades as quais apenas princípios não são capazes de suprimir.

Devido a suas vulnerabilidades, o espaço cibernético se tornou um âmbito perfeito para a prática de diversas condutas ilícitas. Nessa perspectiva, um indivíduo com um pouco de conhecimento na área de informática, é capaz de criar um *vírus* e espalhá-lo para danificar o funcionamento de diversos serviços públicos, como por exemplo, hospitais, estações ferroviárias, tráfego de aeronave. Tais exemplos não se encontram distantes da realidade, tendo em vista o ciberataque ocorrido em 12 de maio de 2017 mediante o *malware WanaCrypt0r.* Mesmo diante divergências entre os pesquisadores do tema, é incerto se um ataque ciberterrorista já se realizou. Contudo, diante situações hipotéticas e mediante um experimento realizado no ano de 2007 pelo Laboratório Nacional de Idaho, é perfeitamente

possível arruinar uma infraestrutura de gerador de diesel através de meios cibernéticos (AYALA, 2016, p. 41-42 *apud* SÁ; MACHADO; ALMEIDA, 2019, p. 106).

Da mesma forma que o terrorismo não apresenta um consenso quanto ao seu conceito, o ciberterrorismo também ostenta certas dificuldades na matéria, obstando a criação de um tipo penal específico para tal conduta. Contudo, diante inúmeras pesquisas acerca do tema, o ciberterrorismo afigura um ataque mediante o uso de aparelhos eletrônicos conectados à *Internet* para a prática de atos ilegais, com o intuito de causar terror e graves prejuízos a um Estado ou em um grande número de pessoas. A diferença entre ciberguerra, cibercrimes e ciberterrorismo é demonstrada a partir dos seus sujeitos ativos e passivos. Na ciberguerra, a agressão cibernética é promovida de Estado para Estado, com o fim de impor seus objetivos e danificar a capacidade do outro. Os cibercrimes, ou crimes cibernéticos, são confundidos com o ciberterrorismo, portanto se difere quanto a motivação, finalidade e extensão do dano que almeja causar, tendo em vista que o cibercrime é motivado pela obtenção de uma vantagem econômica e o ciberterrorismo não, apenas possui o dolo específico de causar um dano de grande proporção por razões políticas ou religiosas através do medo infligido. Os governos mundiais estão atentos quanto a gravidade do tema e já adequaram seus ordenamentos jurídicos para a nova realidade tecnológica. O país pioneiro a realizar alterações em sua legislação foram os Estados Unidos da América, devido ao ataque realizado em 11 de setembro de 2001, adotando medidas de combate ao terrorismo e ciberterrorismo no *Patriot Act.* Nesse sentido, o Reino Unido também passou a coibir e punir através de legislações severas o terrorismo e atos ciberterroristas através do *Terrorism Act* 2000, 2006 e 2008.

No cenário brasileiro, a Constituição Federal de 1988 em seus artigos 4º e 5º, inciso XLIII, reconhecem o repúdio ao terrorismo como um dos princípios básicos das relações internacionais, equiparando-o a crime hediondo, extinguindo a possibilidade de concessão da fiança, graça e anistia. Ademais, as Leis nº 7.170/83, nº 8.072/90 e nº 12.850/13 tratam acerca do tema e punem os atos terroristas. Ainda, o Brasil ratificou ao menos 15 convenções e protocolos que abordam o combate ao terrorismo. Entretanto, uma lei específica se fez necessário para tipificar a conduta terrorista, consoante requereu o mandado de criminalização implícito no artigo 5º, inciso XLIII da Carta Magna. Além disso, uma lei específica era almejada para tratar da questão do ciberterrorismo, tendo em vista o meio em que atua, sendo diverso do terrorismo convencional.

Assim, o legislador pátrio, empenhando-se a aprimorar o ordenamento jurídico no que dispõe a Constituição, bem como nivelar-se à política antiterrorista estrangeira, submeteu ao Congresso Nacional o Projeto de Lei nº 2.016/15 que se tornou a Lei Ordinária nº

13.260/2016, conhecida como Lei Antiterrorismo. Não obstante, a Lei Antiterrorismo apresenta características de um Direito Penal do Inimigo, uma teoria concebida por um doutrinador alemão, que traz como princípios basilares da teoria a insegurança e o medo. Assim, a Lei relativiza direitos, tendo um perfil de tutela penal punitiva e preventiva, ferindo alguns princípios constitucionais previstos. Contudo, apesar da Lei ter previsto de forma ínfima a conduta ciberterrorista, é meritório o avanço apresentado no ordenamento.

O melhor enquadramento da conduta de ciberterrorismo é tipificado no §1º, inciso IV do artigo 2º, evidenciando o dolo específico de gerar o pânico generalizado com um rol exemplificativo. Além disso, referido artigo traz conceitos próximos dos abordados no presente trabalho, ou seja, define o ciberterrorismo pela finalidade do ato, que é intimidar ou coagir governos ou sociedades, em prol de objetivos políticos, religiosos ou ideológicos. A primeira aplicação efetiva da Lei foi com a Operação *Hashtag*, por meio da qual foram punidos oito suspeitos por seus atos preparatórios, de um suposto ataque terrorista que iria ocorrer durante as Olímpiadas sediadas no Brasil em 2016. Porém, além de tipificar as condutas que possam interferir contra o Estado, é necessário a criação e manutenção de meios que inibem a ameaça virtual. Com a presente junção, resguardará a soberania brasileira frente a ataques praticados no país ou a aqueles praticados além dos limites territoriais. A nível adicional, necessária é a atuação em conjunto com outros Estados-Nações com intuito de regular o ciberespaço através de um órgão, da qual os países-membros seriam intermediadores (ÁVILA, 2014, p. 54).

Por ora, é reconhecido o avanço legislativo a partir da elaboração de uma Lei Federal que tipifica condutas de terrorismo e, de forma breve, do ciberterrorismo. Contudo, críticas pairam sobre a Lei, tais como a lesão da ordem constitucional do Estado brasileiro, uma vez que afronta princípios previstos na Carta Magna, tais como isonomia e presunção de inocência, sendo defendido que não deve haver um Direito Penal para cidadãos e outro excepcional para supostos inimigos. Desse modo, compreensível o entendimento de que a legislação carece de reforma, bem como de maior debate com a doutrina penalista.

Referências

ALCÂNTARA, Bruna Toso de. Brasil e Ciberterrorismo: desafios para o Rio 2016. **The Ninth International Conference on Forensic Computer Science - ICoFCS**, [S. l.], p. 84-89, 2015. Disponível em: http://icofcs.org/2015/papers-published-011.html. Acesso em: 20 ago. 2019.

ALESSI, Gil. Justiça condena oito réus da Operação Hashtag por "promover Estado Islâmico". **EL PAÍS.** São Paulo, 04 maio. 2017. Disponível em: https://brasil.elpais.com/brasil/2017/05/04/politica/1493929233_074812.html. Acesso em: 12 out. 2019.

ALMEIDA, Débora de Souza de *et al*. **Terrorismo**: comentários, artigo por artigo, à Lei 13.260/2016 e Aspectos Criminológicos e Político-Criminais. 1. ed. Salvador: JusPodvim, 2017. 384 p.

ANDRADE, Andressa Paula de. **Dogmática penal sem ofensa ao bem jurídico? Os atos preparatórios de Terrorismo na Lei 13.260/2016.** Dissertação (Mestrado em Ciência Jurídica) - Universidade Estadual do Norte do Paraná, Jacarezinho, 2019. Disponível em: https://uenp.edu.br/pos-direito-teses-dissertacoes-defendidas/direito-dissertacoes/12763-andressa-paula-de-andrade/file. Acesso em: 22 ago. 2019.

ÁVILA, Rafael Oliveira de. **Regimes internacionais e poder informacional**: o caso da Netmundial. 2014. 290f. Tese - Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2014. Disponível em: < https://repositorio.ufmg.br/bitstream/1843/BUBD9RFJG5/1/tese_para_impress_o_a_partir_p_g_5.pdf>. Acesso em: 13 maio. 2020.

CALLEGARI, André Luís; LIRA, Cláudio Rogério Sousa. **Direito Penal antiterror: necessidade de definição jurídico-penal para a tipificação de terrorismo no Brasil.** Pensar, Fortaleza, v. 20, n. 3, p. 710-745, pub. set./dez. 2015. Disponível em: https://periodicos.unifor.br/rpen/article/download/3494/pdf. Acesso em: 20 ago. 2019.

CARVALHO, António Augusto Ramos. O Ciberespaço e os novos desafios à Soberania e à Segurança dos Estados. In: SEMINÁRIO INSTITUTO DA DEFESA NACIONAL JOVEM, 5., 2019, Évora. **Anais.** Évora: Instituto da Defesa Nacional e Escola de Ciências Sociais da Universidade de Évora, 2019, p. 221-237.

COSTA, Matheus Souza. **O ciberterrorismo diante o atual ordenamento jurídico brasileiro**. Monografia (Bacharelado em Direito) - Universidade Federal de Lavras, Lavras/MG, 2017. Disponível em: <http://repositorio.ufla.br/handle/1/30772>. Acesso em: 20 ago. 2019.

CURITIBA. Justiça Federal. Sentença. Ação Penal nº 504686367.2016.4.04.7000/PR. Autor: Ministério Público Federal. Réus: Oziris Moris Lundi dos Santos Azevedo; Alisson Luan de Oliveira; Hortencio Yoshitake; Leonid El Ladre de Melo; Luis Gustavo de Oliveira; Fernando Pinheiro Cabral; Israel Pedra Mesquita; Levi Ribeiro Fernandes de Jesus. Juiz: Marcos Josegrei da Silva. Curitiba, 04 de maio de 2017. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/wp-content/uploads/sites/41/2017/05/Evento-613-SENT1.pdf>. Acesso em: 20 out. 2019.

DALLARI, Dalmo de Abreu. **Elementos da Teoria Geral do Estado.** 2. ed. Saraiva: São Paulo, 1998.

EL PAÍS. Ciberataque paralisa 16 hospitais do Reino Unido. Londres, 12 maio. 2017. Disponível em:

https://brasil.elpais.com/brasil/2017/05/12/internacional/1494602389_458942.html?rel=mas. Acesso em: 21 out. 2019.

GAVIÃO, Juliana Venturella Nahas. A proibição de proteção deficiente. **Revista do Ministério Público do Rio Grande do Sul**. Porto Alegre, n. 61, p. 93-111, maio./out. 2008. Disponível em: <http://www.amprs.org.br/arquivos/revista_artigo/arquivo_1246460827.pdf. Acesso em: 19 out. 2019.

GOMES, Rodrigo Carneiro. **Críticas à lei de enfrentamento ao terrorismo e seus avanços**. Revista Consultor Jurídico, 5 de abril de 2016. Disponível em: < https://www.conjur.com.br/2016-abr-05/academia-policia-criticas-lei-enfrentamento-terrorismo-avancos>. Acesso em: 19 out. 2019.

GRECO, Luís. Sobre o chamado Direito Penal do Inimigo. **Revista da Faculdade de Direito de Campos,** ano VI, nº 7, 2005. Disponível em: <http://fdc.br/Arquivos/Mestrado/Revistas/Revista07/Docente/07.pdf>. Acesso em: 22 ago. 2019.

LASMAR, Jorge Mascarenhas. A legislação brasileira de combate e prevenção do terrorismo quatorze anos após 11 de Setembro: limites, falhas e reflexões para o futuro. **Revista de Sociologia e Política**, Curitiba, v. 23, n. 53, p. 47-70, mar. 2015 . Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-44782015000100047&lng=en&nrm=iso>. Acesso em:12 maio. 2020.

MASSON, Cleber. **Direito Penal Esquematizado**: Parte Geral. 9ª ed., vol. 1. Rio de Janeiro: Forense; São Paulo: Método, 2015. 1071 p.

MELO, Emanuel André Ré de. **O Cibercrime como móbil para a prática de atos terroristas.** Dissertação (Mestrado em Direito: Especialidade em Ciências Juridico-Forenses apresentada à Faculdade de Direito) - Faculdade de Direito da Universidade de Coimbra, Coimbra, 2017. Disponível em: <https://eg.uc.pt/handle/10316/84128>. Acesso em: 22 ago. 2019.

PONTE, Antonio Carlos da; KAZMIERCZAK, Luiz Fernando. Terrorismo: Análise da Lei nº 13.260/16. **Revista Jurídica da Escola Superior do Ministério Público de São Paulo**, 2017. Disponível em: < http://www.esmp.sp.gov.br/revista_esmp/index.php/RJESMPSP/article/view/345>. Acesso em: 29 ago. 2019

RODRIGUES, Gabriel Gean. **Análise da lei 13.260/16 (Lei Antiterrorismo) e seu impacto no Direito Penal**. Monografia (Especialização em Inteligência de Segurança Pública) - Universidade do Sul de Santa Catarina, Palhoça, 2017. Disponível em: <https://www.riuni.unisul.br/handle/12345/4792>. Acesso em: 19 out. 2019.

SÁ, Alan Oliveira de; MACHADO, Raphael Carlos Santos; ALMEIDA, Nival Nunes. O encontro da guerra cibernética com as guerras eletrônica e cinética no âmbito do poder marítimo. **Revista da Escola de Guerra Naval**., Rio de Janeiro, v. 25, n. 1, p. 89-128. janeiro/abril. 2019. Disponível em: < https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/797>. Acesso em: 12 maio. 2020.

SOUZA, João Edson de. **Direito penal e terrorismo**: regime penal e persecutório no Brasil e Portugal. Dissertação (Mestrado em Direito: Especialidade em Ciências Jurídicas) - Universidade Autônoma de Lisboa, Lisboa, 2019. Disponível em: <http://repositorio.ual.pt/handle/11144/4282>. Acesso em: 19 out. 2019.

TANGERINO, Dayane Fanti. O papel do Estado no combate ao ciberterrorismo. **Canal Ciências Criminais,** [s.l], 13 jul. 2016. Disponível em: < https://canalcienciascriminais.com.br/o-papel-do-estado-no-combate-ao-ciberterrorismo/>. Acesso em: 10 maio. 2020.

TERRORISM ACT 2006, **Legislation.Gov.Uk**. [s. l. : s. n]**,** 20--?. Disponível em: http://www.legislation.gov.uk/ukpga/2000/11/section/1. Acesso em: 03 ago. 2019.

THE UNITED STATES DEPARTMENT OF JUSTICE. **The USA PATRIOT Act: Preserving Life and Liberty**. Disponível em: https://www.justice.gov/archive/ll/highlights.htm. Acesso em: 03 ago. 2019.

Data de recebimento: 03.06.2020
Data de aprovação: 08.08.2020