
**Matheus Souza Costa**

# O Ciberterrorismo diante do atual ordenamento jurídico brasileiro.

**Lavras - MG**
**2017**

**MATHEUS SOUZA COSTA**

# O Ciberterrorismo diante do atual ordenamento jurídico brasileiro.

Monografia apresentada à Universidade Federal de Lavras, como parte das exigências do Curso de Direito, para a obtenção do título de Bacharel.

Prof. Dr. Ricardo Augusto de Araújo Teixeira
Orientador

**Lavras - MG**
**2017**

**MATHEUS SOUZA COSTA**

# O Ciberterrorismo diante do atual ordenamento jurídico brasileiro. Cyberterrorism in the face of the current Brazilian legal system.

Monografia apresentada à Universidade Federal de Lavras, como parte das exigências do Curso de Direito, para a obtenção do título de Bacharel.

APROVADA em 25 de janeiro de 2018
Dra. Débora Cristina de Carvalho, UFLA

Prof. Dr. Ricardo Augusto de Araújo Teixeira
Orientador

**Lavras - MG**
**2017**

## AGRADECIMENTOS

Aos meus pais, Jonas e Elessandra pelo amor e apoio incondicional, em todas as minhas decisões nas diferentes etapas da minha vida, e ao meu irmão Vinícius.

Ao meu avô Francisco e avós Célia e Ziloca, por todo zelo e carinho que os avós podem depositar em seus netos. Vocês sempre recarregavam minhas energias e me enchiam de esperança.

A minha tia Silvana, por ser minha segunda mãe e sempre ser estar pronta para me ajudar a qualquer momento que eu precisasse.

A minha Tia Raquel, Tia Ana e Tia Maria por me irradiar de palavras boas.

Aos meus cachorros, Toby, Fred e Mel. Fontes inesgotáveis de amor.

A minha namorada, Fabiana, pelo companheirismo, amor, apoio em todos os momentos e singular torcida.

A todos professores que fizeram parte da minha vida. Em especial a Tia Jane, professora da minha 1ª série, por ter me ajudado em um momento crítico da minha vida. A Tia Helô, professora da minha 3ª e 4ª séries pelas magníficas aulas de artes. A Tia Márcia, professora da minha 3ª e 4ª séries, que sempre foi um exemplo de guerreira e hoje aí de cima deve estar muito orgulhosa dessa minha conquista. A Dona Maria, professora de matemática da minha da 5ª a 8ª série, por sempre ser gentil e meiga, deixando minhas manhãs mais alegres. A prof. Gisele de literatura e redação da minha 5ª serie ao 2º ano do ensino médio, por me ensinar o prazer pela leitura. A prof. Eva de geografia do meu 3º ano pelas caronas e altas conversas. A prof. Marita de química do meu 3º ano, por ser extremamente humana ao compreender que nem todos são bons em exatas, valorizando e reconhecendo o esforço que eu fazia para tentar entender a matéria. A prof. Débora, minha primeira orientadora na UFLA, por ter me acolhido e me ensinado a dar os primeiros passos nesse novo ambiente que estava me inserindo. A prof. Silvia, por ser mais que uma professora excelente e ter me ajudado a desembaraçar partes dos meus conflitos internos. A prof. Daniela por toda ajuda na publicação do meu primeiro artigo científico. A prof. Fernanda, por todo carinho materno que teve com a minha turma. Ao prof. Ricardo, por ter sido meu orientador nesse trabalho e ter me ajudado nessa empreitada. E por último, mas não menos importante, a minha mãe por ser a MELHOR professora de história de todos os tempos, que eu tive a honra de ter aula por sete anos seguidos, da minha 5ª serie ao 3º ano do ensino médio, fonte da minha inspiração e motivo por eu acreditar que eu posso tentar melhorar o mundo.

## RESUMO

O Ciberterrorismo é um ataque a sistemas de computadores, informações, programas de computadores e/ou dados, que tem o intuito de intimidar ou coagir governos ou sociedades em busca de objetivos políticos, religiosos ou ideológicos. Além disso, esses ataques são potencialmente capazes de causar e espalhar pânico em toda a população, que se torna refém do medo, já que seus resultados são imprevisíveis, fazendo com que seja, inclusive, uma ameaça ao Estado Democrático de Direito. Em vista disso, temos um problema em relação à questão sobre como o ordenamento pátrio deveria ser utilizado perante a um ataque de ciberterrorismo. Logo, objetivo geral desse estudo é conhecer a dinâmica do ciberterrorismo e como deve o ordenamento jurídico brasileiro abordar a tal ato. Ademais, será feita uma feita uma análise de uma eventual legitimidade para aplicação da Lei Antiterrorismo (nº 13.260, de 16 de março de 2016) de caráter emergencialista. Para isso, marco teórico adotado foi a cibernética de segunda ordem e o método de pesquisa utilizado foi o bibliográfico, tendo o levantamento de informações realizado a partir de livros, artigos e publicações na internet. Destarte, tal reflexão acerca destes ataques é um campo aberto para o estudo e aprofundamento no tema, sendo necessária uma abordagem que seja adequada ao seu grau de periculosidade, emergencilidade e extensão dos danos, com os direitos fundamentais da nossa pátria.



**Palavras-chave:** Direito Penal. Crimes Digitais. Ciberterrorismo.

**ABSTRACT**

Cyberterrorism is an attack on computer systems, information, computer programs and / or data, which is intended to intimidate or coerce governments or societies in pursuit of political, religious or ideological goals. In addition, these attacks are potentially capable of causing and spreading panic throughout the population, which becomes hostage to fear, since its results are unpredictable, making it even a threat to the Democratic Rule of Law. In view of this, we have a problem with the question of how the patriot order should be used in the face of an attack of cyberterrorism. Therefore, the general objective of this study is to know the dynamics of cyberterrorism and how the Brazilian legal system should approach such an act. In addition, a cover of an analysis of a possible legitimacy for application of the Antiterrorism Law (nº 13.260, of March 16, 2016) of an emergency character. For this, the theoretical framework adopted was the second order cybernetics and the research method used was the bibliographical one, having the information gathered from books, articles and publications on the internet. Thus, such reflection on these attacks is an open field for the study and deepening in the subject, being necessary an approach that is adapted to its degree of dangerousness, emergencility and extension of the damages, with the fundamental rights of our homeland.

**Keywords:** Criminal Law. Digital Crimes. Cyberterrorism.

**SUMÁRIO**

# 1. INTRODUÇÃO

A Internet provocou muitas mudanças rápidas em nossos hábitos, tradições e cultura, pois, ajudaram a promover uma comunicação rápida e instantânea entre as mais longínquas regiões. Entretanto apesar dos benefícios que o uso da internet proporcionou, ela apresenta muitas vulnerabilidades, e com isso, novos tipos de condutas ilícitas começaram a ser praticadas, tendo algumas, inclusive, danos imensuráveis e podendo trazer caos a um Estado, e por isso, termos como Guerra da Informação, Cibersegurança, Ciberguerra e Ciberterrorismo ganharam espaço em vários ordenamentos jurídicos de diversos Estados.

Dessa forma, o Ciberterrorismo, como lembra Moreira (2004), foi utilizado pela primeira vez por Barry Collin, na década de 80, sendo uma consequência da convergência entre o terrorismo e o ciberespaço, de tal modo, que o ciberespaço seja o meio para fins terroristas. Em vista disso, tem como finalidade gerar efeitos psicológicos à população civil, que se torna refém do medo, já que seus resultados são imprevisíveis, fazendo com que seja, inclusive, uma ameaça ao Estado Democrático de Direito.

Entretanto, temos um problema em relação à questão sobre como o ordenamento pátrio deveria ser utilizado perante a um ataque de ciberterrorismo. Logo, objetivo geral desse estudo é conhecer a dinâmica do ciberterrorismo e como deve o ordenamento jurídico brasileiro abordar a tal ato. Além disso, será feita uma feita uma análise de uma eventual legitimidade para aplicação da Lei Antiterrorismo (nº 13.260, de 16 de março de 2016) de caráter emergencialista. Mais especificamente, objetiva-se: averiguar de forma um breve histórico do terrorismo e suas definições e características; identificar alguns conceitos de ciberterrorismo, seus objetivos, atores, alvos de preferência e tipos de armas utilizadas; examinar as medidas de cibersegurança adotadas em alguns países; caracterizar o estado atual da legislação relativo ao ciberterrorismo; propor uma formulação de qual seria a melhor aplicação.

Para isso, o método de pesquisa utilizado foi o bibliográfico, tendo o levantamento de informações realizado a partir de livros, artigos e publicações na internet. Assim, para o entendimento do marco teórico, temos levar em conta a Cibernética: que é, como lembra Barros (2015), derivado da palavra grega '*kubernetes*' que significa controle, e é uma união entre a relação humana com a informação e com as máquinas de cibernética. Desse modo, segundo Bertalanffy (2010 citado por BARROS, 2015, p. 36), "a cibernética é uma teoria dos sistemas de controle baseada na comunicação (transferência de informação) entre o sistema e

o meio e dentro do sistema, e do controle (retroação) da função dos sistemas com respeito ao ambiente."

Em vista disso, a cibernética se tornou um novo paradigma do pensamento científico, pois, a sociedade passa ser compreendida por um estudo das mensagens e facilidade da comunicação que se encontra ao seu dispor. (WIENER, 1970, p.25.)

Não obstante, segundo Barros (2015), a cibernética hoje se encontra dividida em duas fases, sendo de primeira e segunda ordem. Dessa forma, a cibernética de primeira ordem (1940 a 1975), foi determinada pela caracterização do campo de estudo como um campo passivo, e por isso, voltada para o determinismo linear clássico. Destarte, a cibernética de segunda ordem revolucionou ao trabalhar com questões do ideal da complexidade e da noção de pensamento sistêmico, já que compreende o sistema social uma interação complexa aberta, sem predeterminações.

Portanto, a cibernética de segunda ordem será adotada como marco teórico desse trabalho, que terá como fim a análise do ciberterrorismo de acordo com novas regras complexas, pois, a partir da aplicação da teoria da cibernética, conforme explica Renata Barros (2015, p.41), "uma ação pode causar uma grande reação, nas relações interconectadas pelo mundo virtual da sociedade contemporânea internacional."

Em suma, o ciberterrorismo é um atentado contra a dignidade da pessoa humana, alicerce principal do Estado Democrático de Direito, estabelecido na Constituição de 1988, merecendo atenção devido à atualidade e pela extensão dos danos causados pelo os ataques. Por isso, tal reflexão acerca destes ataques é um campo aberto para o estudo e aprofundamento no tema. Destarte, é necessária uma abordagem, a tal conduta, que seja adequada ao seu grau de periculosidade, emergencilidade e extensão dos danos, com os direitos fundamentais da nossa pátria.

## 2. TERRORISMO

Antes de adentrar na discussão sobre ciberterrorismo, se faz necessário entender o que é o terrorismo. Para tanto, iremos tecer algumas linhas acerca da sua história e as discussões sobre seu conceito e *modus operandi.*

## 2.1. Histórico do Terrorismo

A origem do terrorismo e do provável criador, segundo Dias (2010), é inexistente, já que como a guerra e a corrupção, o terrorismo surgiu sem uma "certidão de nascimento". Entretanto, é viável discutir a campanha terrorista ao observar o contexto histórico da época dos ataques, possibilitando assim, observar as modificações do terrorismo quanto aos seus objetivos.

A primeira ocorrência que merece atenção foi o movimento judeu político-religioso realizados pelos Sicários e Zelotas, que segundo Sean e Stephen (2009 citado por CHAGAS, 2012, p. 12), se revoltaram "contra a dominação romana rejeitando o pagamento de tributo dos israelitas à um imperador pagão, levando à destruição de Jerusalém pelos romanos, do Segundo Templo (por conta da invasão romana) e o suicídio em massa dos zelotas." Além disso, conforme explica Pedro Vilela:

> A história dos Sicários e Zelotes é uma progressão de elementos políticos e religiosos e uma Judéia ocupada. A rejeição zelote ao domínio estrangeiro, a ideia de uma Israel livre sob a vontade divina, a rejeição ao ideário pagão e a honra na morte pelo divino, cumulado ao empobrecimento da população rural e desestruturação da sociedade tradicional, causada pela administração romana, construiu o cenário necessário para o surgimento de um grupo radical como os Sicários. (VILELA, 2014, p. 6).

Desse modo, os primeiros "homens-bomba" para provocar o terror não usavam dinamite, mas sim suas adagas para assassinar.

Ao caminhar mais um pouco pela história, ainda utilizava-se de assassinatos e incêndios com intento de combater e coagir governos julgados opressores, porém, conforme ressalta Vilela:

> Nunca havia sido utilizada a terminologia "terrorismo" para descrever um ato ou ação política. A primeira instância de uso do termo registrada dá-se do período do "Terror" durante a revolução francesa, na época os atos perpetrados pelo governo jacobino (ou período da Convenção) de Robespierre eram chamados de *terrorisme.* (VILELA, 2014, p. 7).

Nesse contexto, temos o considerado terrorismo moderno, que se originou em meados da revolução francesa. Assim,

> Do final de 1800 até o início de 1900, o terrorismo foi usado para descrever as atividades violentas de vários grupos, incluindo organizações de trabalhadores, anarquistas, grupos nacionalistas que se revoltaram contra as potências estrangeiras, e organizações políticas ultranacionalistas. (CHAGAS, 2012, p. 14).

Outro ataque marcante de cunho terrorista desta época, talvez o que gerou mais consequências até hoje, foi o assassinato do arquiduque austríaco Francisco Ferdinando em Saravejo na Bósnia em 28 de julho de 1914, que foi o "pingo no copo de água" que desencadeou a primeira guerra mundial:

> O assassinato do Arquiduque, príncipe herdeiro do Império Austro-Húngaro, repercutiu profundamente na política mundial levando a Áustria-Hungria a declarar ultimato e após guerra a Sérvia, forçando a aliada Rússia a declarar hostilidade a Austria-Hungria ocasionando a Primeira Grande Guerra. (VILELA, 2014, p. 9).

A segunda guerra mundial, entretanto, segundo White (2012 citado por CHAGAS, 2012, p. 14), mudou novamente o significado de terrorismo. A ênfase se voltou para os grupos nacionalistas que se revoltavam contra a dominação européia no mundo. Contudo, apenas após a Revolução Iraniana de 1979 que surgiu o entendido atualmente como terrorismo religioso, já que mudou a estrutura do terrorismo, com a utilização de ferramentas, como o terrorismo suicida dos homens-bomba, que amplificavam o sentimento de terror. Destarte, segundo White (2012 citado por CHAGAS, 2012, p. 16), o terrorismo, até então, era visto como um conflito subnacional.

O que evento que mudou esse cenário e elevou o patamar do terrorismo pra um assunto global, foi o ataque que a Al Qaeda realizou contra os Estados Unidos, dentro de seu território, no dia 11 de setembro de 2001. Assim, como conta Vilela (2014, p.14) "o grupo jihadista Al-Qaeda preparou e realizou o maior atentado terrorista da história, com quase 3.000 mortos e 10 bilhões de dólares em danos estruturais, contra a mais poderosa nação do globo, os Estados Unidos da América." Desse modo:

> Foi a partir desta data que o terrorismo fundamentalista islâmico passou a receber tamanha, senão, quase que total atenção. E deste então, a palavra "terrorismo" passou a ser relacionada (pelos ocidentais) aos acontecimentos desta data e à fé islâmica em sua forma fundamentalista. (CHAGAS, 2012, p. 14).

Ademais, este ataque gerou uma série de consequências:

> Estes ataques teriam efeitos profundos na forma como nos protegeríamos e combateríamos o terrorismo: primeiramente, além de declarada a Guerra ao Afeganistão, também havia sido declarada "Guerra ao Terror", à criação da utilização de todos os meios disponíveis do estado para o combate ao terrorismo; secundariamente, é criada a lei do *Patriot Act* que aumenta os poderes do executivo para tomar decisões sem a necessidade de intervenção do judiciário ou legislativo. Com a criação do *Patriot Act* e a adoção da "Guerra ao Terror" o sistema americano começa a criar um sistema de vigilância e controle que permitiria a prisão de indivíduos baseados na suspeição (muitas vezes racial ou religiosa) ou possibilidade de futuras violações. (VILELA, 2014, p. 14 e 15).

O nosso cenário atual se encontra nesta fase de terrorismo pós moderno, cuja violência se tornou global e as velhas regras da diplomacia, guerra e estadismo surtem pouco efeito diante destes ataques. (CHAGAS, 2012). Logo, após o atentado do 11 de setembro houve uma criação de novas políticas que visam conter o terrorismo, e é sobre essas novas políticas que iremos debruçar nesse trabalho, para poder entender a definição, as características e os meios que os ordenamentos políticos se utilizam para se proteger contra o terrorismo e propor quais seriam os mais adequados para o ciberterrorismo.

## 2.2. Conceito e o *Modus Operandi* do Terrorismo

O conceito de terrorismo é eivado de ambivalências, tanto é polissêmico como errático. Assim segundo Chagas (2012, p. 17), "não existe um conceito universal justamente pelo mesmo possuir diferentes raízes e motivações." O fato de haver uma dificuldade para se conceituar as condutas terroristas implicam em um problema para o Direito Penal, conforme explica Callegari e Lira:

> De fato, há uma dificuldade de se conceituar as condutas terroristas. E esses problemas de significado são de extrema importância para o Direito Penal, já que não se permite a criação de crimes *ah doc*, dada a necessidade de se estabelecer uma clara fronteira de atuação da norma penal antiterror, a partir de condutas (pré)determinadas, com preceitos primários e secundários expressos e taxativos. (CALLEGARI; LIRA, 2015, p. 718).

Dessa forma, várias são as tentativas de se tentar criar ou suplementar as deficiências do conceito de terrorismo. O primeiro significado dado ao termo "terrorismo", conforme foi apontado no tópico anterior por Vilela (2014, p. 7), e melhor explica por Laqueur (2001 citado por CHAGAS, 2012, p. 17 e 18) "foi em 1798, descrito pelo dicionário da Academia Francesa como sistema ou regime de terror." Depois disso, inúmeras foram as tentativas de diversos autores, nos séculos seguintes, para estabelecer um conceito claro de terrorismo. Vejamos alguns esforços a seguir.

Na perspectiva de Andrade (1999 citado por DIAS, 2010, p. 2), que tem por base o entendimento do FBI, o "terrorismo é o uso ilícito de violência contra pessoas ou bens para intimidar ou coagir um governo, a população civil ou parte dela, para alcançar objectivos políticos ou sociais."

Entretanto, para Waldron (2010 citado por VILELA, 2014, p. 20) tal definição mostra-se insuficiente, já que o ataque terrorista nem sempre deseja ocasionar uma reação na vítima (Estado ou população), pois, é possível que tenha objetivos distintos e variados.

Não obstante, Chomsky (2004, p. 190), ao criticar a política contra terrorista norte americana, demonstra que antes do ataque do 11 de setembro de 2001, o termo terrorismo era entendido da seguinte forma por um manual do Exercito americano: "o uso calculado de violência ou ameaça de violência para alcançar metas de natureza política, religiosa ou ideológica... por meio da intimidação, coação ou instalação do medo.'" O autor apresenta uma conceituação que embora indique que a violência utilizada pelo terrorismo deve ser com o cunho intimidatória para incutir o terror, é bastante imprecisa por não ter como delimitar quais são as metas, podendo ser as mais diversas possíveis.

Para Saint-Pierre o terrorismo busca atingir mais uma eficácia simbólica do que estratégica ou tática, conforme as palavras de Chagas (2012, p. 18) ao citar o pensamento do referido autor, o “terrorismo é uma maneira de fazer política através (da ameaça ou) do uso da violência, procurando através desta, atingir um resultado no nível psicológico do indivíduo, e que algumas vezes utiliza-se de atos genocidas para conseguir tal resultado.” Interessante notar neste conceito que nem sempre o uso da violência real precisa acontecer, basta um ameaça ao um blefe que condicione para os objetivos do terrorista, para que já possa ser considerado terrorismo.

Já para Viriato Dias (2010, p. 2) ao analisar alguns conceitos de terrorismo, conclui que as definições “convergem numa premissa comum: o terrorismo é uma violência criminosa que visa, além do mais, criar terror nos dirigentes políticos, militares e o medo na população civil.”

Por fim, ao analisar a história do terrorismo e alguns conceitos, segundo Teixeira (2017) é possível estabelecer um ponto comum: o terrorismo é negação das soluções políticas. Pois o terrorismo apresenta diversas causas, sendo elas a fundamentalista (de cunho religioso), a nacionalista (unidades separatistas), a ideológica (movimentos sociais que tornam radicais) e de Estado (Estado contra a população com intenção de subjugá-la). Logo, independente da face que o terrorismo adota os seus atores não estão abertos para diálogos e as velhas regras políticas da diplomacia. Por isso, quando se tem um ataque terrorista, a parte praticante do ato já abriu mão das soluções políticas e realmente acredita que essa atitude mais drástica é única que ira conduzir para os seus fins. Nesse sentido:

> Os ataques terroristas são políticos. Os grupos terroristas, por não terem poder para travar uma guerra contra unidades estatais, procuram atingir objetivos políticos desestabilizando governos por meio de ações que disseminam o medo e a insegurança entre as populações. Os grupos terroristas islâmicos procuram, também, atingir os países muçulmanos com governos ligados de algum modo ao Ocidente, tentando fortalecer grupos internos de oposição a esses governos. (AGUILAR, 2011, p. 11).

Destarte, a dificuldade para encontrar um conceito para as condutas terroristas tem relação também com o *modus operandi* do terrorismo, pois:

> O fato é que os atos geralmente considerados como "terroristas" não possuem uma forma pré-definida pelas diversas organizações terroristas em atividade no mundo. Isso implica na constatação de que o *modus operandi* dos grupos terroristas são diversos e dinâmicos, modificando-se de acordo com o cenário social, a finalidade a ser atingida e os meios necessários para obter os resultados. (CALLEGARI; LIRA, 2015, p. 728).

Em uma análise mais detalhada, Neto (2002 citado por FIGUEIREDO; RAMOS, 2012, p. 203 e 204) traça algumas características sobre o *modus operandi* do terrorismo, denominados por ele de princípios básicos, que contribuem para o sucesso e aumento do poder de destruição dos ataques terroristas:

> a) O princípio da surpresa: Atacar onde e quando menos se espera; b) O princípio do alvo certo: A escolha correta do alvo a ser atingido é determinante na promoção do medo e do terror; c) O princípio das externalidades: Valorizar não apenas o ato terrorista, mas, sobretudo, os efeitos de curto, médio e longo prazos das ações do terror; d) O princípio da tragédia: Quanto maior o número de vítimas, melhor. Vítimas para chocar é o preceito básico das ações terroristas; e) O princípio do efeito moral: Abater moralmente os inimigos, disseminando o medo e o pavor entre a população;
> f) O princípio das novas possibilidades: Sempre prometer novos ataques caso suas exigências não sejam cumpridas; g) O princípio da presença onipotente: Estar presente em qualquer lugar, em todo lugar, sempre disposto a agir, se for preciso; h) O princípio da ameaça latente: Tornar-se uma ameaça sempre presente na vida das pessoas, países e regiões; i) O princípio da eficiência destruidora: Sua eficiência e sua competência, mesmo a serviço do mal, são objetos de admiração; j) O princípio da redenção: A morte de seus seguidores é o ingresso na vida eterna; k) O princípio do exército de reserva: Divulgar adesões em massa ao movimento terrorista e deixar claro que "o que não falta são terroristas dispostos a morrer"; l) O princípio da onipresença: Fazer crer aos inimigos que dispõe de um exército de terroristas prontos para a ação em seu próprio território; m) O princípio do simbolismo destrutivo: Valorizar o efeito simbólico das ações. Destruir símbolos que significam poder, riqueza e intransigência; n) O princípio da martirização: Transformar seus adeptos em mártires; o) O princípio da espetacularização: Fazer de seus atos verdadeiros espetáculos de destruição;
> p) O princípio do catastrofismo: Sempre prometer a anunciar uma tragédia maior; q) O princípio da inversão: Transformar a vítima em algoz; r) O princípio do estímulo à guerra total (o princípio da "jihadização"): Promover a guerra santa. Transformar os conflitos locais em choques de civilizações;
> s) O princípio da demonização: Seu inimigo é visto como o Grande Satã, causador de todos os males do mudo; t) O princípio da invisibilidade: Ser um inimigo invisível, sem cara nem movimentação; u) O princípio do anonimato: Cometer atos mantendo-se no anonimato; v) O princípio da reflexão induzida: Pelos atos praticados contra alvos cuidadosamente escolhidos, induz-se à reflexão: por que este ou aquele país foi escolhido como alvo das ações terroristas?; w) O princípio da bola da vez: Deixar seus inimigos pensarem que um deles será a próxima vítima a alvo do terror; x) O

> princípio do silêncio: Manter-se em silêncio para não se expor. (NETO, 2002, p. 60-62)

Em derradeiro, este trabalho não pretende esgotar tamanha discussão, mas apenas constatar a dificuldade em ter um tipo penal especifico para os ataques terrorista. Logo, como assevera Teixeira (2017), os dogmas da legalidade e da tipicidade cerrada tem se mostrado insuficientes para enfrentar um tipo de criminalidade excepcional. O que nos leva a indagar se a reafimarção desse direito de fundo liberal e ainda positivista conseguiria de fato dar uma solução neste caso ou se talvez seria mais eficaz encontrar uma alternativa fora do direito penal clássico.

## 3. ESPAÇO CIBERNÉTICO

Após a assimilação sobre as discussões apresentadas no tópico anterior, é preciso entender o que seria o espaço cibernético, pois, este é o ambiente onde ocorrem os ataques de ciberterrorismo, sendo diferente do espaço físico, que é onde ocorre o terrorismo "convencional", o que leva uma sistemática diferente para o entendimento destes fenômenos.

A partir da década de 1970, ocorreu uma enorme multiplicação de instrumentos tecnológicos destinados à comunicação, resultando em nova forma de interação humana: a Cibernética, que seria uma teoria dos sistemas de controle baseada na comunicação dos homens através das máquinas.

Por conseguinte, a cibernética de segunda ordem é a que melhor conduz essa nova forma de interação, pois, trabalha com questões do ideal da complexidade e da noção de pensamento sistêmico, já que compreende o sistema social uma interação complexa aberta, sem predeterminações. Além do que, a partir da aplicação da teoria da cibernética, conforme explica Renata Barros (2015, p.41), "uma ação pode causar uma grande reação, nas relações interconectadas pelo mundo virtual da sociedade contemporânea internacional."

O uso da internet, hoje a principal plataforma para acesso ao espaço cibernético, que é o ambiente onde se desdobra as inter-relações homem-máquina, se deu, inicialmente, e de forma intensa, por organizações militares e nas universidades nos anos 70, entretanto, já nos anos 90 houve um grande crescimento no número de usuários e também na quantidade e diversidade de conteúdos aí presentes, se tornando, então segundo Batista, Ribeiro e Amaral (2004), um ambiente complexo, tal qual o mundo, já que nele ocorrem mudanças a todo o momento e estas são divulgadas instantaneamente, por isso, uma lógica linear baseada na ideia de causa e efeito não faz sentido neste ambiente.

Desse modo, a internet conforme explica Batista, Ribeiro e Amaral (2004), pode ser entendida como uma rede de comunicações transnacional que possibilita a troca de informação e aquisição de bens e serviços. Além disso, provocou muitas mudanças rápidas em nossos hábitos, tradições e cultura. Ela ajudou, a promover uma comunicação rápida e instantânea entre as mais longínquas regiões, de maneira a facilitar o contato entre as pessoas, e por isso, conforme ensina Marshall McLuham (1989), inserindo-as em uma Aldeia Global, não mais circunscritas à suas condições geográficas, mas com um ponto comum: o Ciberespaço ou espaço cibernético.

No âmbito acadêmico, existem diversas definições de ciberespaço, cada uma com uma abordagem e perspectiva diferente. Não obstante, é possível encontrar um núcleo comum a essas definições. Para tanto é necessário voltar à origem: A palavra "*cyberspace*", segundo Levy (1998 citado por CHAGAS, 2012, p. 31), foi primeiramente designada em 1984, por William Gibson, um escritor de ficção científica. Ademais, o ciberespaço, segundo Levy (1998 citado por CHAGAS, 2012, p. 31), constitui um campo vasto, aberto, ainda parcialmente indeterminado.

Em vista disso, define Kuehl:

> Um domínio operacional dentro do ambiente de informação cuja distinta e única característica é enquadrada pelo uso de eletrônicos e espectros eletromagnéticos para criar, armazenar, modificar, trocar e explorar informações via redes interdependentes e interconectadas usando tecnologias de informação/comunicação.[1] (KUEHL, 2009, tradução nossa)

Nesse sentido, elucida Gardini (2014, p. 10), o ciberespaço "é um ambiente virtual de comunicação, transmissão e armazenagem de dados que pode ser acessado nos mais diferentes dispositivos eletrônicos conectados por redes eletromagnéticas." Outrossim, segundo LEÃO (2003 citado por CHAGAS, 2012, p. 32):

> O ciberespaço é explorável e visualizável em tempo real. O ciberespaço engloba: as redes de computadores interligados no planeta (incluindo seus documentos, programas e dados); as pessoas, grupos e instituições que participam dessa interconectividade e, finalmente, o espaço (virtual, social, informacional, cultural e comunitário) que se desdobra das inter-relações homem-máquina.

Em suma, trata-se de um ambiente sem fronteiras, onde as mudanças são mais velozes que as do mundo físico, sendo então, um espaço em que os indivíduos estão de certo

[1] Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.

modo fora do controle do Estado, estes, no entanto, não podem evitá-lo, pois, seu uso tornou-se essencial.

Desse modo, o ciberespaço, como afirmado, é de grande importância aos Estados, já que, segundo Barros (2015, p. 83) este "pode lhes ajudar na atuação, no âmbito das relações internacionais, pela busca da dominação da informação, no espaço cibernético e, também, em outros domínios, que se encontram fora do mundo cibernético." Trata-se, então, de uma nova forma de poder, uma nova maneira de afetar os diferentes sujeitos das relações estabelecidas nas relações internacionais.

Portanto, a partir do exposto, depreende-se que o ciberespaço é um novo local de domínio de guerra, tal qual são a terra, o mar, o ar e o espaço. Trata-se de uma nova área para conduzir a política internacional, e:

> Sendo um novo domínio com facilidade de acesso, baixo custo, capaz de mudanças rápidas e a oportunidade de anonimato, o ciberespaço se torna interessante para Estados, organizações, instituições e até indivíduos, especialmente no que diz respeito ao poder no contexto internacional. (GARDINI, 2014, p. 13).

Em vista disso, além destes "atrativos" para condutas ilícitas, ele apresenta muitas vulnerabilidades, e com isso, novos tipos de condutas ilícitas começaram a ser praticadas, tendo algumas, inclusive, danos imensuráveis e podendo transformar um Estado em caos. Nesse sentido:

> É, portanto, grande a dificuldade de se fiscalizar e exigir que os Estados e demais atores internacionais obedeçam às normas de Direito Internacional no domínio cibernético e, consequentemente, não ajam forma de viabilizar a violação de direitos, no mundo real. (BARROS, 2015, p. 83 -84).

Desta forma, com utilização cada vez mais frequente do ciberespaço nas mais diversas áreas, a utilização para fins terroristas vem ganhando destaque nas academias, e isso explica o porquê do surgimento de termos: Guerra da Informação, Cibersegurança, Ciberguerra e Ciberterrorismo, vem ganhando espaço nos ordenamentos jurídicos de vários países.

## 4. CIBERTERRORISMO

O que aconteceria, conforme expõe Chagas (2012), se as comportas de uma hidrelétrica fossem abertas de maneira simultânea por uma pessoa não autorizada? E se houvesse uma invasão no sistema de alguma torre de controle de tráfego de aeronaves? Ou se os semáforos da cidade de São Paulo fossem desligados por determinado tempo? E se um

indivíduo invadir um sistema de controle de um fabricante de cereais e modificar os níveis de certa substancia no alimento, causando intoxicação em massa e até mesmo a morte de algumas crianças que consumirem este produto? Ou se um ciberterrorista, através de um vírus, conseguir invadir os sistemas de comando de uma usina nuclear no Irã?

Diante de tais hipóteses de danos imensuráveis, que temos que as primeiras notícias sobre o ciberterrorismo são datadas de 1990 quando, segundo Weimann (2004 citado por CHAGAS, 2012, p. 28), "o rápido crescimento do uso da internet e o debate sobre a sociedade da informação provocaram vários estudos sobre riscos potenciais enfrentados pela alta conectividade em rede e pela alta tecnodependência dos Estados."

Desse modo, conforme elucida deColarik e Janczewski (2008 citado por CHAGAS, 2012, p. 28), o termo ciberterrorismo foi utilizado pela primeira vez a partir da reunião do G8, no fim de 1990, onde foram analisados e discutidos os crimes promovidos via aparelhos eletrônicos ou a disseminação de informações pela internet. Nesse sentido:

> A interligação da sociedade com a tecnologia e o aumento da dependência pela mesma deu ao terrorismo a oportunidade de explorar novos recursos; e consequentemente, foi crescendo o receio de que frutos de deficiências tecnológicas tornasse possível a execução de ataques ciberterroristas. (CHAGAS, 2012, p. 29).

Em vista disso:

> O que propiciou o surgimento de ações características do ciberterrorismo decorreu da evolução dos primeiros vírus criados para atacar computadores e redes, isto é, ataques de hackers com a finalidade de roubar informações e espionar segredos comerciais. (MENEZES, 2017, p. 20).

Destarte, temos que observar a discussão acerca de um ataque de ciberterrorista nunca ter ocorrido. Segundo John J. Klein (2015, p.28, tradução nossa) "nenhuma instância de ciberterrorismo real foi registrada. Até à data, não houve nenhuma instância registrada de ciberterrorismo em instalações públicas dos EUA, sistemas de transporte, usinas de energia nuclear, redes elétricas ou outros componentes importantes da infra-estrutura nacional."[2] Desse modo, Klein (2015) expõe que para muitos estudiosos sobre o assunto esse medo da ameaça de um ataque ciberterrorista é exagerado, e acrescenta que:

> Muitos especialistas em segurança informática não acreditam que seja possível usar a Internet para causar dano, lesão ou morte em grande escala. Alguns desses especialistas observam que os sistemas informáticos críticos são resistentes ao ataque através dos investimentos de tempo, dinheiro e experiência durante a concepção e desenvolvimento desses sistemas críticos. Por exemplo, o Departamento de Defesa dos Estados Unidos, a Agência

[2] No single instance of real cyberterrorism has been recorded. To date, there has been no recorded instance of cyberterrorism on U.S. public facilities, transportation systems, nuclear power plants, power grids, or other key components of the national infrastructure.

> Central de Inteligência e o Federal Bureau of Investigation são relatados para proteger seus sistemas mais críticos ao isolar - também chamados de "poupança de energia" - da Internet e de outras redes internas de computadores.[3] (KLEIN, 2015, p. 28 – 29, tradução nossa).

Nesse sentido, Gardini (2014) também entende nunca ter havido um ataque ciberterrorista, já que não houve um ataque deste tipo que causasse a mesma sensação de pânico que o 11 de setembro foi capaz, em suas palavras:

> Até o momento, não houve um ataque suficientemente destrutivo ou perturbador por meio do ciberespaço que causasse o mesmo sentimento de medo motivado por ataques físicos, como, por exemplo, um evento como o 11 de setembro, onde 19 terroristas sequestraram quatro aviões de passageiros, sendo dois deles jogados contra as torres do World Trade Center em Nova Iorque, o que resultou na morte de quase 3 mil pessoas. (GARDINI, 2014, p. 19).

Entretanto há estudiosos que apontam que já houve tentativas de ataques ciberterrorista e até mesmo ataques já efetuados. Para Cícero Neto e Matheus Santos (2014, p. 229) ocorreu uma tentativa em 2010, sendo "um caso de grande repercussão internacional foi a utilização de um "Vírus", denominado Stuxnet, com intuito de invadir usinas nucleares, como as do Irã e na Índia."

Já Chagas (2012) nos trás o caso da Estônia. Segundo a autora o país passou por três semanas de ataques motivados emocionalmente pela:

> Remoção da estátua de bronze de um soldado soviético do centro de Tallinn, a capital do país, para transportá-la para um cemitério militar. O governo russo e estonianos descendentes de russos pronunciaram-se contra a mudança, e estes últimos iniciaram um protesto onde 150 pessoas ficaram feridas. Segundo a Rússia, a estátua é uma homenagem àqueles que lutaram contra o nazismo, mas os estonianos a veem como um símbolo da ocupação soviética. Esses ataques deixaram diversos sites inacessíveis, incluindo os do parlamento, ministérios, bancos e páginas de notícias, abalando a economia local em razão da inacessibilidade de instituições importantes (como bancos e empresas); e impossibilitando até que os membros do governo se comunicassem por email, pois estes ataques foram direcionados aos servidores de instituições que são responsáveis pela a infraestrutura da internet do país. (CHAGAS, 2012, p. 41).

Assim, nos conta Chagas (2012) que autores como Tikk, Kaska e Vihul, consideram tal ocorrido como um exemplo de ciberterrorismo. Ademais, a possibilidade de usar a

[3] Many computer security experts do not believe that it is possible to use the Internet to inflict damage, injury, or death on a large scale. Some of these experts note that critical computer systems are resilient to attack through the investments of time, money, and expertise during the design and development of these critical systems. For example, the U.S. Department of Defense, Central Intelligence Agency, and Federal Bureau of Investigation are reported to protect their most critical systems by isolating—also called airgapping— them from the Internet and other internal computer networks.

tecnologia para realizar esses ataques é real, sendo comprovado por um experimento realizado em 2007 no Idaho National Laboratory, conforme explica Barney Warf e Emily Fekete:

> No entanto, existe a possibilidade de usar tecnologia para causar destruição. Um experimento realizado em 2007 no Laboratório Nacional de Idaho mostrou que é possível destruir uma infra-estrutura através do uso de computador por hackers em um ambiente controlado. O "teste Aurora" permitiu que os hackers fossem sancionados pelo governo dos EUA para penetrar um gerador diesel de US $ 1 milhão e 27 toneladas de 100 milhas até o ponto em que o gerador efetivamente explodiu (Rid & McBurney, 2012). Um vídeo do experimento mostrando que o gerador tremendo e fumando vazou para fontes de notícias meses depois e ainda pode ser visualizado on-line no YouTube (http://www.youtube.com/watch?v=fJyWngDco3g).[4] (FEKETE; WARF, 2016, p. 147, tradução nossa).

Não obstante, em 2017, hospitais na Inglaterra tiveram seus atendimentos prejudicados por um ataque de um vírus (*malware*) de resgate, conhecido como *WanaCrypt0r*, que é uma variação do vírus *WCry/WannaCry*. Para tanto os criminosos alegaram que queriam certa quantia para fornecer uma chave que fosse possível restaurar os dados e sistemas do hospital.

> Representantes de hospitais públicos afetados na Inglaterra relataram ao jornal que cancelaram atendimentos e redirecionaram ambulâncias para outros hospitais. De acordo com o "New York Times", ao menos 16 instituições sofreram, simultaneamente, um bug em seus sistemas de informação. Não há evidências de que os dados de pacientes tenham sido afetados, segundo a "BBC". (G1, 2017).

Tal ataque atingiu vários países como

> Em território russo, foram atingidos os computadores do Ministério do Interior e os sistemas de estação ferroviária e de instituição bancária. Em solo francês, a empresa automobilística Renault suspendeu a produção por medida de segurança. Na Alemanha, também foi prejudicado o sistema cibernético da rede ferroviária. O Brasil, neste panorama, não restou ileso: o Instituto Nacional do Seguro Social (INSS), no Rio de Janeiro, e a Petrobrás interromperam, como medida de segurança, suas atividades. No Tribunal de Justiça e no Ministério Público de São Paulo a rotina também foi abalada com a retirada de seus respectivos sites do ar e com o desligamento preventivo de equipamentos informáticos. (ALMEIDA; CUNHA, 2017).

Dessa forma, como já citado acima, o *Ransomware WanaCrypt0r* funciona da seguinte forma:

> Em linhas gerais, este malware, que pode se alastrar para outros computadores ligados em rede, criptografa os arquivos do disco rígido que

[4] However, the possibility of using technology to cause destruction does exist. An experiment conducted in 2007 at the Idaho National Laboratory showed that it is possible to destroy infrastructure through the use of computer hacking in a controlled environment. The “Aurora test” successfully allowed hackers sanctioned by the US government to penetrate a $1million, 27 ton diesel generator from 100 miles away to the point where the generator effectively blew up (Rid & McBurney, 2012). A video of the experiment showing the generator shaking and smoking was leaked to news sources months later and can still be viewed online on YouTube (http://www.youtube.com/watch?v=fJyWngDco3g).

> contém as extensões doc., docx., xls., pps., entre outras, alterando-os para a extensão .WNCRY. Após infectado, surge na tela a mensagem, disponível em vários idiomas, de que os dados foram criptografados e que a descodificação só poderá ser feita pelos autores do ataque. Para tanto, a vítima é constrangida, sob pena de ver seus dados destruídos, a efetuar o resgate no prazo máximo de 7 dias, sendo que terá até o 3º dia para que o quantum exigido não dobre. O meio de pagamento exigido foi bitcoins, moeda digital de difícil rastreamento e utilizada para fins de financiamento de terrorismo. Contudo, o FBI, alerta que o pagamento do resgate não assegura que os dados criptografados sejam recuperados. (ALMEIDA; CUNHA, 2017).

Caso semelhante ocorreu no Brasil quando em Unidades do Hospital do Câncer de Barretos (SP) nas cidades de Jales (SP) e Fernandópolis (SP) sofreram um ataque cibernético no dia 27 de junho de 2017. Os criminosos pediram dinheiro (300 dólares em *bitcoins*) para liberar o sistema. Conforme a reportagem do G1 nos conta:

> Em Fernandópolis, segundo o hospital, a unidade que faz exames preventivos está parada. Ao todo, 150 pacientes vão deixar de ser atendidos. Em Jales (SP), o sistema também foi afetado. Por telefone, o diretor geral do Hospital do Câncer, Henrique Prata, disse que mais de três mil pacientes vão ser prejudicados, já que não há como acessar nenhum tipo de informação. (G1, 2017).

Apesar desses eventos acima descritos não serem um ato de ciberterrorista, já que não tem como saber se a intenção dos criminosos eram só pegar uma quantia em dinheiro ou gerar o pânico e tentar subordinar o Estado a uma vontade política deles, demonstra que tais ataques podem ocorrer a qualquer momento, já que existe aparato tecnológico que possibilite isso.

Isto posto, apesar da incerteza de ter ou não ocorrido um ataque ciberterrorista até hoje, temos um trabalho de Michael L. Gross, Daphna Canetti e Dana R. Vashdi publicada no *Journal of Cybersecurity* da *Oxford University Prass* sobre um estudo para saber se a exposição ao ciberterrorismo letal e não letal afeta o bem-estar psicológico da população e causa esfeitos semelhantes ao terrorismo convencional. Para tanto, foram feitos três estudos entre 2013 e 2016. Nestes estudos os sujeitos assistiram videos clips que expõem ao ciberterrorismo simulado letal e não-letal. Suas descobertas foram as seguintes:

> Nossas descobertas demonstram um estresse baseado no "efeito ciberterrorista". A exposição ao ciberterrorismo não é benigna e compartilha muitos traços com o terrorismo convencional: estresse, ansiedade, insegurança, preferência pela segurança sobre a liberdade, uma reavaliação da confiança nas instituições públicas, uma maior percepção de risco e apoio a políticas governamentais enérgicas. No domínio cibernético, isso se traduz em apoio a políticas como a vigilância da Internet, a regulamentação governamental da Internet e uma resposta militar poderosa ao ciberterrorismo (incluindo retaliação convencional e cinética). Essas atitudes

> podem afetar a tolerância e a confiança necessárias para uma sociedade civil vibrante. Este efeito está associado ao ciberterrorismo não letal que causa perda econômica, bem como com o ciberterrorismo que causa morte e lesões.[5] (CANETTI; GROSS; VASHDI, 2017, p. 49, tradução nossa).

Por isso, levanto em conta os dados levantados por essa pesquisa de Canetti, Gross e Vashdi e os casos acima apresentados, discordamos de Klein (2015) quando este aponta que o medo de uma ameaça de um ataque ciberterrorista é exagerado. Pois, conforme pondera Weimann (2014, p. 11, tradução nossa) "Assim como os eventos do 11 de setembro surpreendeu o mundo, um grande ataque virtual também poderia. A ameaça do ciberterrorismo pode ser exagerada e manipulada, mas não podemos negar nem ousar ignorá-la."[6]

O medo de um ataque ciberterrorista não somente existe, e não é exagerado, como tende a aumentar, conforme aponta André Miceli, professor do MBA de Marketing Digital da Fundação Getulio Vargas (FGV) (2017 entrevistado por Felipe Payão, 2017), em entrevista uma concedida sobre o aumento de *gadgets* na Internet das Coisas:

> Nos próximos anos, certamente veremos a explosão do número de elementos conectados. Bombas de insulina, cardioversores, marca-passos estarão conectados. Aceleradores e pilotos-automáticos de automóveis, controles de casa como aparelhos de ar-condicionado e fogões também. Teremos mais oportunidades para invasões e certamente os criminosos vão aproveitá-las para fazer dinheiro.

Ademais, conforme defende Chagas (2012, p. 39) "qualquer possibilidade de danos à vida humana é de responsabilidade do Estado, que visa garantir o bem estar de sua população." Assim, os Estados que possuem suas estruturas vitais conectadas a rede através de computadores, precisam investir em segurança tecnológica e de um sistema dentro ordenamento jurídico que seja capaz não somente de punir essas condutas, como evitar os danos.

Desse modo, iremos nos debruçar em uma análise mais específica do ciberterrorismo que será dividida entre: conceito, objetivos, atores, armas utilizadas, alvos de preferência e uma distinção entre cibercrime, ciberterrorismo e guerra cibernética. Assim, ao entender o que

---

[5] Our findings demonstrate a stress based 'cyber terrorism effect'. Exposure to cyberterrorism is not benign and shares many traits with conventional terrorism: stress, anxiety, insecurity, a preference for security over liberty, a reevaluation of confidence in public institutions, a heightened perception of risk and support for forceful government policies. In the cyber realm, this translates into support for such policies as Internet surveillance, government regulation of the Internet and a forceful military response to cyberterrorism (including conventional, kinetic retaliation). These attitudes may impinge upon the tolerance and confidence necessary for a vibrant civil society. This effect is associated with non-lethal cyberterrorism that causes economic loss as well as with cyberterrorism that causes death and injury.

[6] Just as the events of 9/11 caught the world by surprise, so could a major cyberassault. The threat of cyberterrorism may be exaggerated and manipulated, but we can neither deny it nor dare to ignore it.

é e como funciona o ciberterrorismo ficará um pouco mais fácil entender como combatê-lo, por meio de medidas de segurança, e como o Direito Penal seria mais eficaz diante desta ameaça.

## 4.1. Conceito

A definição de ciberterrorismo não é uniforme, vez que vários são os conceitos trabalhados por diferentes autores. A respeito disso o primeiro conceitos apresentado é de Amanda Parker, que conceitua ciberterrorismo como:

> Um ato ou ações criminais premeditadas, de natureza política, social ou religiosa, contra informação, sistemas de computadores, programas de computadores e/ou dados que resultem em violência ou danos severos contra civis, por grupos sub nacionais ou agentes clandestinos.[7] (PARKER, 2009, p. 245-246, tradução nossa).

Já Dorothy Denning (2002 citado por GARDINI, 2014, p. 18) trabalha com outro conceito de ciberterrorismo, que seria:

> Um ataque ou ameaça de ataque baseado em um computador com intenção de intimidar ou coagir governos ou sociedades em busca de objetivos políticos, religiosos ou ideológicos. O ataque deve ser suficientemente destrutivo ou perturbador para gerar medo comparável à de atos físicos de terrorismo. Ataques que levam à morte ou lesão corporal, falta de energia prolongada, acidentes de avião, contaminação da água, ou grandes perdas econômicas seriam exemplos. [8]

Nesse sentido, observamos que Denning e Parker convergem para uma definição de ciberterrorismo semelhante, sendo que a de Denning parece ser mais completa. No entanto, segundo Gardini (2014, p. 18), ambas concordam que ciberterrorismo seria "ações de objetivos políticos ou religiosos que são realizadas por meio do espaço cibernético para causar graves danos contra a sociedade civil ou governos".

Não obstante, nota-se, também, que nem toda ação terrorista cometida no ciberespaço é considerada ciberterrorismo. Nessa lógica, explica Lachow (2009, p. 2, tradução nossa): "ciberterrorismo se refere aos meios utilizados para realizar os ataques, não à natureza dos alvos de um ataque terrorista 'clássico'"[9] Dessa forma, o ciberterrorismo utiliza-

---

[7] A premeditated criminal act or actions; political, social or religious in nature, against information, computer systems, computer programs, and/or data which results in violence against or severe harm caused to civilians, by sub - national groups or clandestine agents.

[8] A computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. ...Attacks that disrupt nonessential services or that are mainly a costly nuisance would not [be cyber terrorism].

[9] Cyber terrorism refers to the means used to carry out the attacks, not to the nature of the targets of a "classical" terrorist attack.

se de um meio diferente do utilizado pelo terrorismo, considerado clássico, para espalhar o terror na sociedade.

Ainda, temos o conceito dado por Lima (2006 citado por CHAGAS, 2014, p. 18), que diz que:

> O ciberterrorismo é uma extensão natural do terrorismo, e que este se aproveita da dependência que a sociedade tem da tecnologia, em especial da internet. E por esse tipo de terrorismo, assim como os demais, planeja os atos motivados por alguma razão (ideológica, política, religiosa, etc.). Esse tipo de terrorismo pode funcionar desde atos de disseminação de vírus ao público quanto à execução de ataques maiores.

Por fim, há de se destacar um último conceito que é dado por Bill Nelson:

> O ciberterrorismo é a destruição ou desrupção ilegal da propriedade digital para intimidar ou coagir governos ou sociedades na busca de objetivos políticos, religiosos ou ideológicos. Como um subconjunto do terrorismo, o ciberterrorismo envolve o uso da informação como arma, método ou alvo, para alcançar objetivos terroristas. O ciberterrorismo existe dentro e além do ciberespaço e inclui destruição física de qualquer dispositivo, sistema de dispositivos ou processo com um componente de informação. No menor denominador comum, um componente de informação pode ser entendido como representando o código binário. Os atos levados a perturbar, negar o serviço, destruir e corromper código binário são, portanto, atos de ciberterrorismo. Uma característica do ciberterrorismo é a sua capacidade de alavancar meios baratos para obter efeitos desproporcionais através da destruição, negação, engano, corrupção, exploração e ruptura. O ciberterrorismo pode aumentar a destruição, ou a perturbação, do ato, permitindo uma maior cobertura, efeito e eficiência do alvo. O ciberterrorismo pode aumentar ou apoiar o terrorismo tradicional, ou ser empregado como uma forma distinta de ação em seu próprio direito. [10] (NELSON, 1999, p. 9-10, tradução nossa).

Em suma, percebe-se que apesar de cada autor trabalhar seu próprio conceito de ciberterrorismo, ele pode ser entendido, de uma forma geral, conforme esclarece Chagas (2012) como um ataque a sistemas de computadores, informações, programas de computadores e/ou dados, ou seja, um ataque a um fator tecnológico por outro fator tecnológico, realizado por um ciberterrorista (feitor do ciberterrorismo). Esta transgressão tem o intuito de intimidar ou coagir governos ou sociedades em busca de objetivos políticos,

[10] Cyberterrorism is the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological. As a subset of terrorism, cyberterror involves using information as a weapon, method, or target, to achieve terrorist goals. Cyberterror exists in and beyond cyberspace and includes physical destruction of any device, system of devices, or process with an information component. At the lowest common denominator, an information component can be understood to represent binary code. Acts taken to disrupt, deny service, destroy, and corrupt binary code are thus acts of cyberterror. A characteristic of cyberterror is its ability to leverage inexpensive means to gain disproportionate effects through destruction, denial, deceit, corruption, exploitation, and disruption. Cyberterror can increase the destructiveness, or disruptiveness, of the act by enabling greater target coverage, effect, and efficiency. Cyberterror may augment or support traditional terrorism, or be employed as a distinct form of action in its own right.

religiosos ou ideológicos. Além disso, esses ataques, que geralmente não possuem um padrão, devem ser potencialmente capazes de causarem e espalharem o medo e pânico em toda a população, o que nos leva para a análise do próximo tópico que irá demonstrar os objetivos do ciberterrorismo.

## 4.2. Objetivos

Os ataques ciberterroristas, como lembra Batista, Ribeiro e Amaral (2004), têm intenções políticas, religiosas ou ideológicas, e seus objetivos são causar danos graves e imensuráveis, como por exemplo: perda de vida, prejuízos econômicos, corte de energia elétrica ou água. Nesse sentido, o ciberterrorista tem objetivos mais gravosos que o cibercriminoso comum, nas palavras de Collin (1997), ele age para que uma "nação não seja capaz de comer, beber, mover-se ou viver"

Por isso, esta forma de terrorismo, segundo Denning (2000), trata-se de ataques feitos para intimidar ou coagir um governo ou seu povo em prol dos objetivos sociais e/ou políticos almejados pelo ciberterrorista.

Nesse sentido, segundo Batista, Ribeiro e Amaral (2004, p.34), esse ataque tem como "objetivo desestabilizar política, ideológica ou financeiramente um grupo, organização ou governo, utilizando a internet para perpetrarem as ações consideradas necessárias."

Já segundo Marco Aurélio Gonçalves Pinto:

> A natureza do Ciberterrorismo pode ter em vista: (1) Destabilizar Estados soberanos para alcançar uma maior forca de influencia numa certa região; (2) Causar uma visibilidade internacional para problemas persistentes como e o caso da Palestina, de forma a conseguir maior afecto; (3) Retaliar contra Estados soberanos em certas regiões que são encarados como sendo inimigos; (4) Minar a influencia de forcas mais poderosas que estejam a operar na região. (PINTO, 2011, p. 39).

Ademais, os objetivos do ciberterrorismo são simbólicos e mortíferos, e a sua repercussão pelos meios de comunicação social potencializam os efeitos pretendidos por esse ataque, de forma a causar e espalhar pânico e terror na sociedade, um dos outros principais objetivos do ciberterrorismo.

Entender os objetivos do ciberterrorismo se mostra relevante, pois os objetivos estão intimamente ligados com uma possível tipificação deste ataque, já que os objetivos são o que "separam" o ciberterrorismo de um cibercrime comum, através de um dolo específico, o que justificaria que a aplicação de um enquadramento em um cibercrime comum seria insuficiente para esta conduta.

## 4.3. Atores do ciberterrorismo

Os praticantes de atos característicos do ciberterrorismo são conhecidos como ciberterroristas. E podem ser grupos criados para a prática do ciberterrorismo, ou derivados de grupos terroristas. Nesse sentido, Marco Aurélio Gonçalves Pinto, em sua tese de mestrado, defende que:

> Os Ciberterroristas são normalmente jovens do sexo masculino, alguns com habilitações acadêmicas elevadas (Mestrados ou Doutoramentos), que tem a consciência de estar a violar a lei desrespeitando as normas sociais, a ordem e os sistemas de controle social. Eles diferem dos criminosos comuns em pelo menos quatro características fundamentais: (1) Efetuam crimes de forma mais violenta; (2) Tem como meta infligir medo numa população alvo enorme; (3) Servem uma agenda social enorme tentando recrutar mais elementos para a causa deles; (4) Tentam conseguir uma exposição máxima aos medias. (PINTO, 2011, p. 39).

Ainda, segundo Batista, Ribeiro e Amaral (2004, p.34), acreditam-se que alguns tipos de atores podem realizar atividades típicas de ciberterrorismo, como: "Hackers (amadores ou profissionais), grupos criminosos (grupos terroristas) e sub estados (motivados por objetivos políticos)."

Ressalta-se que os atores do ciberterrorismo não devem ser confundidos com os do hacktivismo, que é:

> Um termo usado por estudiosos para descrever a união entre hacking com ativismo político. Embora politicamente motivado, o hacktivismo difere-se do ciberterrorismo, por visar protestar e destruir ou atrapalhar o funcionamento de sites, fóruns, etc., mas, não visa matar, ferir fisicamente ou aterrorizar. (CHAGAS, 2012, p. 30).

Em suma, percebe-se que tal ataque não é realizado por pessoas comuns, já que exige um conhecimento profundo sobre informática. Isso evidência o dolo na conduta, pois, um atentado deste porte, além de ser planejado com muita antecedência, demonstra de fato as reais intenções do sujeito, que passou anos estudando para usar todo conhecimento adquirido para fins de desestabilizar o Estado e gerar pânico.

## 4.4. Armas utilizadas

O ciberterrorismo tem algumas formas, como por exemplo: vírus, cavalo de troia, *worms, spywares* e SPAM. Essas formas são meios iniciais de ciberataque, e são utilizados, porque possuem uma grande capacidade de difusão no meio tecnológico. Entretanto, a característica do ciberterrorismo é difundir o pânico, terror ou medo a fim de atingir grande quantidade de pessoas. Assim, somente os vírus, cavalo de troia, *worms, spywares* e SPAM, não são capazes de sozinhos provocarem o pânico na sociedade, uma vez que é necessário que

o ciberterrorismo, ao realizar um ataque, tenha o dolo de causar medo, terror ou pânico nos sujeitos. Nesse sentido, somente quando os vírus e demais formas, forem utilizados para causarem pânico em massa é que eles poderão ser considerados como armas do ciberterrorismo.

Dessa forma, as armas utilizadas pelo ciberterrorismo são diferentes do terrorismo convencional, sendo a principal delas a internet. Têm-se, ainda segundo Batista, Ribeiro e Amaral (2004, p.35), alguns tipos de armas, como por exemplo: "armas do tipo convencional, armas lógicas e armas comportamentais".

A definição desses três tipos de armas é dada por Gonçalo Batista, Carlos Ribeiro e Feliciano Amaral. Primeiramente, armas do tipo convencional são aquelas que têm por objetivo atacar:

> Essencialmente, as estruturas físicas dos suportes da informação impedindo a utilização de determinados serviços utilizando para o efeito: Bombas de Impulso Electromagnético – estes dispositivos geram impulsos electromagnéticos que actuam como uma onda de choque do mesmo tipo, provocando danos no alvo semelhantes aos efeitos das descargas eléctricas dos relâmpagos; Munições de Radiofrequência (*RF*) – estas armas podem ser activadas por sinais de rádio e podem adaptar-se a granadas de mão, granadas de morteiro ou de artilharia; Dispositivos Electromagnéticos Transitórios – *TED's* ("*Transient Electromagnetic Device*") para realizarem a monitorização TEMPEST (BATISTA; RIBEIRO; AMARAL, 2004, p.36).

Destarte, estas armas representam um grande perigo, já que podem realizar ataques indetectáveis a grande distância e a vítima pode não se aperceber que está a ser atacada, não havendo medidas disponíveis para proteger um alvo potencial de um ataque. Por isso:

> As armas *RF* e os *TED's* apresentam as seguintes vantagens face às armas convencionais: Têm baixo custo e são resistentes ao tempo; Têm capacidade para atacar instantaneamente alvos únicos ou alvos múltiplos; Não são letais para os seres humanos, desde que devidamente ajustadas. (BATISTA; RIBEIRO; AMARAL, 2004, p.36).

Já as armas lógicas têm por objetivo instalar-se no sistema e desativá-lo:

> Com as Armas Lógicas pretende-se atacar a lógica operacional dos sistemas de informação, introduzindo atrasos ou comportamentos indesejados no seu funcionamento. De acordo com a NSA (*National Security Agency*) dos EUA, os "*hackers*" utilizam as seguintes técnicas para efectuarem os ataques: envio de Vírus Informáticos (que podem ser introduzidos num computador e destruir programas); Bombas Lógicas (que se instalam nos sistemas operativos dos computadores e permanecem em hibernação até receberem um sinal específico que os acciona e que vai despoletar a destruição dos sistemas hospedeiros - "*host systems*"); "*Worms*" (vírus que se propagam de forma independente e destroiem os sistemas operativos); Cavalos de Tróia (proporcionam a entrada de intrusos sem serem percebidos; apesar de aparentemente inofensivos quando são activados têm um elevado poder destrutivo); "*Back Doors*" e "*Trap Doors*" (são mecanismos construídos

> dentro de um sistema para acesso à sua informação num momento posterior à sua instalação); "*Virtual Sit-Ins*" e "*Blockades*" (bloqueio do acesso ao equipamento); "*e-mail Bombs*"; Ataques de Recusa de Serviço ("*Denial of Service Attacks*"), entre outros mecanismos que permitem desligar e destruir sistemas de transmissão de dados e hardware. (BATISTA; RIBEIRO; AMARAL, 2004, p.36-37).

As armas comportamentais são aquelas que visam destruir a confiança que os usuários depositam nos sistemas de informação, bem como influenciar a interpretação da informação que neles circula. Nesse nível, os ciberterroristas se utilizam da decepção e da guerra psicológica. (BATISTA; RIBEIRO; AMARAL, 2004).

Por fim, temos as *botnets*, que segundo Schiller (2007 citado por PINTO, 2011, p. 71), "são centenas ou milhares de computadores comprometidos usados (vendidos ou alugados) para ataques em grande escala." Ademais, as *botnets:*

> São formadas por um vasto numero de computadores comprometidos que estão infectados por código malicioso, e podem ser remotamente controlados através de comandos transmitidos pela Internet. Daí, centenas ou milhares de computadores comprometidos podem operar de forma a disruptir ou a impedir o trafego das vitimas, colher Informação, distribuir *SPAM* e vírus em grande escala, etc. (PINTO, 2011, p. 72).

Em suma, o ciberterrorista possui um arsenal vasto que ligado a sua capacidade e criatividade pode abrir um mundo de centenas de oportunidades que possibilita a criação de um ataque. Isto implica na dificuldade de criar um tipo penal fechado para essa conduta, já que existem variados meios que possibilitam que ocorra uma transgressão deste tipo.

## 4.5. Alvos de preferência

O ciberterrorismo se utiliza dos meios de comunicação social, e principalmente da internet como meio de garantia de maior alcance aos alvos pretendidos, já que a internet não respeita barreiras e divisões políticas ou geográficas, e ainda permite o anonimato a quem prática atos ciberterroristas.

Dessa forma, utilizando-se da internet, os ciberterroristas têm como objetivo de ataque, segundo Batista, Ribeiro e Amaral (2004, p.39), os "programas de gestão e controle dos serviços essenciais de um Estado, provocando a sua paralisação ou até a sua destruição". Algumas estruturas estão incluídas neste programa de gestão, são eles: redes de distribuição elétrica, de água potável e de gás; redes de controle de tráfego aéreo; redes hospitalares; redes bancárias e financeiras; redes governamentais. (BATISTA; RIBEIRO; AMARAL, 2004).

Além disso, vale lembrar que:

> Atualmente, os ciberterroristas mundiais elegeram os EUA e as empresas multinacionais como alvos preferenciais [...] tendo a sua incidência

> aumentado consideravelmente a partir dos atentados de 11 de setembro de 2001. (BATISTA; RIBEIRO; AMARAL, 2004, p.39).

Desse modo, os alvos são as estruturas vitais dos estados e das empresas multinacionais conectadas a rede através de computadores. Logo, com cada vez mais os estados tendo que se modernizarem, estes estão aumentando em grande quantidade a possibilidade de alvos para os ciberterroristas, que caso sofressem um ataque, seriam capazes de instituir uma situação catastrófica, disseminando o medo e o pânico na sociedade.

## 4.6. Distinções entre cibercrime, ciberterrorismo e guerra cibernética

Com o intuito de evitar confusões sobre o objeto deste trabalho, se faz necessário esclarecer a diferença entre os termos cibercrime, ciberterrorismo e guerra cibernética, afim de que fique cristalina a necessidade de uma abordagem jurídica distinta e única ao ciberterrorismo. Para tanto, o conceito de cibercrime pode ser entendido da seguinte maneira:

> O conceito de cibercrime varia de crimes econômicos, como fraude de informática, roubo, falsificação, pirataria informática, espionagem informática, sabotagem, extorsão informática, pirataria e outros crimes contra a propriedade intelectual, a invasão de privacidade, distribuição de conteúdos ilícitos e prejudiciais, o incitamento à prostituição e outros crimes contra a moralidade, e o crime organizado. [11] (MEDERO, 2012, p. 244, tradução nossa).

Posto isto, ciberterrorismo, já elucidado nos tópicos anteriores, possui um dolo específico e se difere de cibercrime no seguinte sentido:

> O ciberterrorismo vai além do cibercrime, mesmo que alguns consideram que ambos são a mesma coisa. Sem dúvida, eles têm alguma conexão porque os terroristas cibernéticos em muitas vezes demsepenham atividades criminosas na rede, mas as causas que os motivam e os benefícios que eles esperam um do outro são diferentes. Ciberterrorismo é a convergência do ciberespaço e do terrorismo, ou seja, "a maneira em que o terrorismo utiliza tecnologia da informação para intimidar, coagir ou para causar danos a grupos sociais e religiosos com fins políticos." Portanto, torna-se desenvolvimentos resultantes de mudar de armas, bombas e mísseis por um computador para planejar e executar ataques que produzem o maior dano possível a civis. Isto implica uma grande diferença em respeito ao cibercrime, o ciberterrorismo procura causar o maior dano possível por razões político religiosas enquanto as ações de cibercrime são direcionados

[11] El concepto de cibercrimen abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el *computer hacking*, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otros crímenes contra la moralidad, y el crimen organizado.

> principalmente para conseguir o benefício econômico.[12] (MEDERO, 2012, p. 244, tradução nossa).

O ciberterrorismo também não se confunde com ciberguerra, já que:

> A ciberguerra pode ser entendida como uma agressão promovida por um estado destinada a danificar severamente as capacidades do outro para impor a aceitação de um objetivo próprio ou simplesmente para roubar informações, cortar ou destruir os seus sistemas de comunicação, alterando suas bases de dados isto é, aquilo que vulgarmente entendido como guerra, mas com a diferença de que o meio empregado não seria violência física, mas um ataque de computador que vai desde se infiltrar em sistemas de computadores inimigos para obter informações para controlar mísseis por computadores, passando por planejamento de operações, gestão de abastacimento.[13] (MEDERO, 2012, p. 244, tradução nossa).

Em suma, parece que a diferença entre ciberterrorismo e outros cibercrimes e seria em relação a questão do elemento subjetivo do agente (motivação e finalidade), bem como a extensão do dano a que almeja. Dessa forma, fica evidente a necessidade de um tratamento diferenciado ao ciberterrorismo de cibercrime pelo direito penal. Portanto, depois de todo o exposto nos tópicos anteriores, devido às diversas facetas que um ataque ciberterrorista pode ter, parece ser impossível criar um tipo penal fechado para esta conduta. Talvez a maneira mais desejável de lidar com tal situação seria a construção de um tipo penal mais aberto, que tivesse algum rol exemplificativo de condutas que conduzissem a devida leitura do dispositivo, para que os aplicadores do direito através da hermenêutica penal pudessem identificar condutas, que mesmo não sendo idênticas as do rol exemplificativo, caracterizariam uma ação ciberterrorista. Ademais teria que haver uma evidencia em relação à diferença do dolo de um ciberataque comum para um atentado ciberterrorista, já que este último exige um dolo específico.

---

[12] El ciberterrorismo va más allá de la ciberdelincuencia, por mucho que algunos consideren que ambos son una misma cosa. Indudablemente tienen cierta vinculación, porque em muchas ocasiones los ciberterroristas desempeñan actividades delictivas en la red, pero la causa que las motivan y los beneficios que esperan unos y otros son diferentes. El ciberterrorismo es la convergencia del ciberespacio y el terrorismo, es decir, "la forma en la que el terrorismo utiliza las tecnologías de la información para intimidar, coaccionar o para causar daños a grupos sociales con fines políticos-religiosos". Por tanto, viene a ser la evolución que resulta de cambiar las armas, las bombas y los misiles por una computadora para planificar y ejecutar unos ataques que produzcan los mayores daños posibles a la población civil. Esto implica una gran diferencia respecto al cibercrimen, el ciberterrorismo busca originar el mayor daño posible por razones político religiosas mientras que las acciones del cibercrimen están dirigidas a conseguir un beneficio principalmente económico.

[13] La ciberguerra puede ser entendida como una agresión promovida por um Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento.

## 5. CIBERSEGURANÇA

Dada a gravidade da matéria, nesta seção iremos abordar as medidas que os governos mundiais estão implementando para se proteger destes ataques ciberterroristas, minimizando os efeitos e danos, através da criação de órgãos específicos para proteção, sistemas de vigilância e, até mesmo, como estão transformando seus ordenamentos jurídicos para essa nova realidade.

Dessa forma, cada vez mais os países estão se equipando com órgãos específicos que são responsáveis pela segurança cibernética do país. Assim, Medero em sua pesquisa aponta alguns exemplos:

> Nos Estados Unidos, por exemplo, o "Critical Infrastructure Assurance Office" (CIAO) e o National Infrastructure Protection Center (NIPC) foram criados para salvaguardar ataques cibernéticos contra redes de infra-estrutura e sistemas nacionais; na Argentina, o Escritório de Coordenação de Emergências em Redes Teleinformáticas é a unidade que tem competência em tudo relacionado à segurança dos sistemas de informação; na China, o Exército Popular de Libertação criou o Centro de Guerra da Informação para dirigir ações em relação à guerra cibernética; no Japão, o governo estabeleceu uma equipe antiterrorista composta por cerca de 30 especialistas em informática e chefe do Escritório de Segurança do Governo, na Espanha, é o Centro Criptológico Nacional, anexado ao Centro Nacional de Inteligência, e dentro dele a "Computer Emergency Response Team" (CERT), responsável por supervisionar a segurança cibernética do país. A missão é estudar a segurança de redes e computadores para prestar serviços de resposta a vítimas de ataques informáticos, publicar alertas de ameaças e vulnerabilidades e fornecer informações para ajudar a melhorar a segurança desses sistemas.[14] (MEDERO, 2012, p. 252, tradução nossa).

Interessante notar também que a OTAN criou em Tallin, Estônia, um Centro de Excelência para a Cooperação em Defesa Cibernética, e conforme demonstra Medero (2012, p. 253, tradução nossa), tem como objetivo "estudar ataques cibernéticos e determinar as circunstâncias em que devem ativar o princípio da defesa mútua da Aliança Atlântica."[15]

---

[14] En EE.UU, por ejemplo, se creó la "Critical Infrastructure Assurance Office" (CIAO) y National Infrastructure Protection Center (NIPC) para salvaguardar de los ataques cibernéticos las redes de infraestructuras y los sistemas del país; en Argentina, es la Oficina de Coordinación de Emergencias en Redes Teleinformáticas la unidad que tiene competencia en todo lo relacionado con la seguridad de los sistemas de información; en China, el Ejército de Liberación Popular ha constituido el Centro de Guerra de la Información para que dirija las acciones en relación a la ciberguerra; em Japón el gobierno ha establecido un equipo antiterrorista compuesto por unos 30 especialistas informáticos y un responsable de la Oficina de Seguridad del Gobierno, en España es el Centro Criptológico Nacional adscrito al Centro Nacional de Inteligencia, y dentro de él, el "Computer Emergency Response Team" (CERT), el responsable de velar por la seguridad cibernética de la nación. Su misión es estudiar la seguridad de lãs redes y ordenadores para proporcionar servicios de respuesta a las víctimas de ataques informáticos, publicar las alertas relativas a amenazas y vulnerabilidades, y ofrecer información que ayude a mejorar la seguridad de estos sistemas.

[15] Estudiar ciberataques y determinar las circunstancias en las que deben activar el principio de defensa mutua de la Alianza Atlántica.

No Brasil não existe um único órgão específico e centralizado para combater e prevenir o terrorismo internacional. (LASMAR, 2015). Porém, o ciberterrorismo fica a encargo do Comando do Exército/Ministério da Defesa em seu Centro de Defesa Cibernética (CDCiber). (LASMAR, 2015).

Se faz mister a análise dos sistemas de controles que os países estão usando para identificar as tentativas destes ataques. Para Batista (2004, p. 49) trata-se de uma verdadeira guerra de informação defensiva. O primeiro sistema que merece destaque é o Echelon, que é segundo Medero (2012, p. 253, tradução nossa) "é um sistema automatizado de intercepção global de transmitido pelos serviços de inteligência de cinco países: Estados Unidos, Grã-Bretanha, Canadá, Austrália e Nova Zelândia."[16] Seu funcionamento, como explica Menezes (2012), se da por meio de localizar várias interceptações eletrônicas em satélites ou outro tipo de onda que transmite informação, como celulares e rádio por exemplo. Depois disso, através do sistema Elchelon a estação ira selecionar, por meio de palavras-chaves, as palavras consideradas perigosas para a segurança nacional. Ademais, os países que integram esse sistema fornecem dicionários de palavras chaves para que possa ser incorporado como filtros automáticos aos aparelhos de interceptação de comunicações e, conforme aponta Batista (2004, p.49), "Esta rede é formada por 120 satélites com capacidade para interceptar e decifrar 189 milhões de mensagens electrónicas por hora."

O próximo sistema de controle interessante é o "Carnivore", que já foi usado pelo FBI. Tal sistema captura emails suspeitos e de interesse da agencia e inclusive, conforme aponta Menezes (2012), especula-se que esse sistema é capaz de espionar o disco rígido do usuário considere suspeito, sem deixar o rastro de sua atividade. Para tanto, ele funcionava da seguinte forma:

> Para isso, um chip é colocado no equipamento dos provedores de serviços de Internet para controlar todas as comunicações eletrônicas que ocorrem através deles, então, quando encontrar uma palavra-chave, que sim com a aprovação do tribunal, ele verifica todos os dados do eletrônico que circula pelo computador da pessoa, acompanha as visitas que eles fazem aos sites da rede e as sessões de bate-papo em que participa. Isto, juntamente com o controle dos endereços IP e dos telefones de conexão, permite a detecção do que eles consideram "movimentos suspeitos" na rede.[17] (MEDERO, 2012, p. 255, tradução nossa).

[16] Un sistema automatizado de intercepción global de trasmisiones operado por los servicios de inteligencia de cinco países: Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda.

[17] Para ello, se coloca un chip en los equipos de los proveedores de servicios de Internet para controlar todas las comunicaciones electrónicas que tienen lugar a través de ellos, así cuando encuentra una palabra clave, eso sí con el visto bueno de la corte, revisa todos los datos del correo electrónico que circulan por el ordenador de esa persona, rastrea las visitas que hacen a sitios de la red y las sesiones de chat en las que participa. Esto junto con el control de las direcciones de IP y de los teléfonos de conexión, permite la detección de lo que consideran "movimientos sospechosos" en la red.

Contudo, este sistema tinha uma falha como aponta Batista (2004, p. 49), “se as mensagens estiverem encriptadas, já é mais difícil ou até impossível, nos casos de chaves mais complexas.”

Nesta mesma linha está o programa "Dark Web", porém, este sistema se foca em atividades terroristas. Este projeto desenvolvido pelo Laboratório de Inteligência Artificial da Universidade do Arizona, funciona da seguinte forma:

> Utilizam técnicas como o uso de "aranhas" e análise de links, conteúdo, autoria, opiniões e multimídia para encontrar, catalogar e analisar atividades de extremistas na rede. Uma de suas ferramentas é o Writeprint, que extrai automaticamente milhares de recursos multilingues, estruturais e semânticos para determinar quem está criando conteúdo "anônimo" online. Na medida em que você pode examinar um comentário postado em um fórum da Internet e compará-lo com escritos encontrados em outros lugares da rede e, além disso, ao analisar esses recursos, você pode determinar com mais de 95% de precisão se o autor tiver produzido outros no passado. Portanto, o sistema pode alertar os analistas quando o mesmo autor produz novos conteúdos, bem como o local onde eles estão sendo copiados, vinculados ou discutidos. Mas a Dark Web também usa um software complexo de rastreamento de páginas, que usa aranhas de tópicos de pesquisa e outros conteúdos para encontrar os cantos da Internet, onde as atividades terroristas estão ocorrendo cabo.[18] (MEDERO, 2012, p. 256, tradução nossa).

Além disso, existem outros sistemas de controle como o OSEMINTI, utilizado pela Espenha e França, o Sintel, que é utilizado pela Esapanha e o FISC que é utilizado pelo governo norte americano para checar as atividades do FBI e da NSA. (MEDERO, 2012).

Portanto, nos resta claro que hoje em dia uma uma generalização desta prática. O que demosntra  que esta havendo resultados efetivos destes sistemas, que ajudam a dectectar ciberterroristas e cibercriminosos. Entretanto, a retenção destes dados é enxergado como uma problema:

> O raciocínio baseia-se no fato de que a retenção de dados (que pode apontar detalhes muito precisos sobre a vida privada de uma pessoa) e o acesso às mesmas pelas autoridades competentes implica uma séria interferência nos

[18] Utilizan técnicas como el uso de “arañas” y análisis de enlaces, contenidos, autoría, opiniones y multimedia para poder encontrar, catalogar y analizar actividades de extremistas en la red. Una de sus herramientas es el Writeprint, que extrae automáticamente miles de características multilingües, estructurales y semánticas para determinar quién está creando contenido “anónimos” online. Hasta el punto que puede examinar un comentario colocado en un foro de Internet y compararlo con escritos encontrados en cualquier otro lugar de la red y, además, analizando esas características, puede determinar con más del 95% de precisión si el autor ha producido otros en el pasado. Por tanto, el sistema puede alertar a los analistas cuando el mismo autor produce nuevos contenidos, así como el lugar donde están siendo copiado, enlazado o discutido. Pero el Dark Web también utiliza un complejo software de seguimiento de páginas, para lo que emplea los spiders de los hilos de discusión de búsqueda y otros contenidos con el objetivo de encontrar las esquinas de Internet, en los que las actividades terroristas se están llevando a cabo.

> direitos fundamentais, como respeito por privacidade e proteção de dados pessoais.[19] (SANCHES FRÍAS, 2016, p.22, tradução nossa).

Contudo, tal autor expõe que tal interferência poderia ser justificada, já que a preservação desses dados e sua transmissão respondem a um objetivo de interesse geral: a segurança pública, pois, há uma luta contra a criminalidade que tem consequencias gravíssimas. (SANCHES FRÍAS, 2016). E propões que o União Européia, através de um basilamento da proporcionalidade e razobiliadade tome as seguintes possíveis medidas:

> Propõe-se que a directiva inclua regras rigorosas sobre o período de armazenagem, tendo em conta as diferentes categorias de dados e assegurando a sua protecção contra o acesso e a utilização ilegais. As regras também devem ser estabelecidas para destruir efetivamente os dados, que só podem ser armazenados no território da UE e, portanto, no âmbito do CDFUE e as autoridades que o aplicam. [20] (SANCHES FRÍAS, 2016, p.25, tradução nossa).

Destarte, Sanches Frías (2016, p. 32, tradução nossa), diz que a busca por uma "fronteira entre liberdade e segurança" pode ser pelas "As diretrizes da jurisprudência comunitária podem ser uma boa base para encontrar o equilíbrio entre reivindicações de "liberdade inestimável" e "segurança a todo o custo""[21]

Em relação à adaptação dos ordenamentos jurídicos para essa nova realidade, os Estados Unidos se encontram um passo a frente em relação ao resto do mundo, muito devido ao 11 de Setembro de 2001, que fez com que o governo norte americano tivesse um preocupação maior em reduzir as ameaças de eventuais ataques ciberterroristas. (BATISTA; RIBEIRO; AMARAL, 2004). Nesse sentido:

> 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. (MENEZES, 2012, p.22).

A principal lei feita pelo governo norte americano foi o *Patriot Act*, que além de melhorar as agências norte americanas e combater de forma mais eficiente o terrorismo

---

[19] El razonamiento parte de la base de que la conservación de los datos (que pueden aportar detalles muy precisos de la vida privada de una persona) y el acceso a ellos por las autoridades competentes supone una injerencia grave en los derechos fundamentales, al respeto a la vida privada y a la protección de datos de carácter personal.

[20] Se propone que la Directiva incluya reglas estrictas relativas al periodo de conservación, teniendo en cuenta las distintas categorías de datos, así como garantizar su protección frente a accesos y usos ilegales. Deben indicarse además normas para destruir de forma efectiva los datos, que sólo puedan ser almacenados en el territorio de la UE y por tanto bajo el ámbito de aplicación de la CDFUE y las autoridades que la aplican.

[21] Las directrices de la jurisprudencia comunitaria pueden ser una buena base para encontrar el equilibrio entre las reclamaciones de "la libertad no tiene precio" y "seguridad a toda costa".

doméstico através da criação de medidas práticas que visam o contra terrorismo doméstico como a criação de um fundo, sejam eles para reparação de danos, fazer análises de riscos de quais prédios seriam os alvos mais prováveis e criar obstáculos para isso e para recompensa *whistleblower*, que é para pessoas que tem informações sobre possíveis ataques terroristas.

O *Patriot Act* ainda cria exceção ao "*posse comitatus act*", o que possibilita a ação de forças armadas dentro do território do país, e o confisco e bloqueio sem ordem judicial se possível desde que seja demonstrado razoavelmente o envolvimento de uma pessoa que esta colaborando ou planejando um ataque terrorista.

Destarte, para o combate do ciberterrorismo importante foram as medidas de vigilância criadas por essa lei, como uma maior possibilidade de interceptação de comunicação (qualquer que seja o meio utilizado, como email e ligações telefônicas), maior compartilhamento de informação entre agências de segurança e inteligência e uma permissão que possibilita um atraso na notificação de mandados de *"sneak and peak"*, ou seja, desde que seja aparente a possibilidade de ataque cibernético, o computador de um ciberterrorista poderia ser invadido e vasculhado.

Além disso, apesar dos Estados Unidos serem o país que mais desenvolveu seu ordenamento jurídico nesta questão, ele não é o único:

> Países como a Suécia, Reino Unido e Grécia possuem legislações severas para coibir e punir ações características de ciberterrorismo, ou seja, tais regramentos consideram ser a informação um bem jurídico que deve ser protegido, englobando a aplicação de penas privativas de liberdade e multa pecuniária. (MENEZES, 2012, p.22).

Recentemente a França sofreu menos 10 atentados desde janeiro de 2015, sendo desencadeados pela invasão da redação do Charlie Hebdo. (PRESSE, France, 2016). Diante de tantos atentados a França teve que adequar o seu ordenamento jurídico. Desse modo, o atual presidente Emmanuel Macron sancionou a nova lei antiterrorismo, no dia 30 de outubro de 2017. Com esta lei as forças de segurança ganham mais poder para conseguir realizar buscas e apreensões, restringir a movimentação de suspeitos de ligação com organizações terroristas, irá estabelecer cercos de imigração e alfândega em um raio de 10 quilômetros de estações de trens, aeroportos e outras portas de entrada na França, e até mesmo fechar templos. (FOLHA DE SÃO PAULO, 2017).

Em suma, parece ser evidente que o mundo já esta em alerta para um possível ataque ciberterrorista e já estão tomando medidas efetivas para a sua prevenção, seja por meio de criação de órgãos específicos para proteção, sistemas de vigilância e, até mesmo, estão adequando seus ordenamentos jurídicos para essa nova realidade.

## 6. O ORDENAMENTO JURÍDICO BRASILEIRO E O CIBERTERRORISMO

Após analisar quais são as medidas que os Estados estão tomando para a prevenção de um ataque ciberterrorismo, iremos voltar nossos olhos para nosso ordenamento pátrio, a fim de saber em que situação ele se encontra, se já existe alguma regulação, quais seriam os institutos já criados para tipos penais semelhantes que poderiam ser incorporados para uma devida persecução penal; e se caso o Brasil sofresse um ataque ciberterrorista, nos dias atuais, qual seria o melhor enquadramento para esta conduta. Desse modo, iremos analisar o ordenamento jurídico brasileiro em relação ao terrorismo convencional, para posteriormente realizarmos um estudo mais focado no ciberterrorismo.

Em vigor, temos a Constituição Brasileira de 1988, que em seu:

> Inciso I do artigo 1º como 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 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).

Nesse sentido, a Carta Cidadã em seu art. 4º, VIII, reconhece como um dos princípios básicos das relações internacionais o repúdio ao terrorismo. Além disso, a Constituição em seu art. 5°, inc. XLIII, como lembra Lasmar (2014, p. 57), "operacionaliza esse repúdio ao constituir o terrorismo como um crime hediondo do qual não há a possibilidade de se conceder fiança, graça, anistia ou indulto e dos quais se punem não apenas os autores mas também os mandantes e 'os que, podendo evitá-los, se omiti[ram]'" Por fim, como lembra Callegari e Lira (2015, p. 733), "o legislador constitucional, no inciso XLIV do artigo 5º, ratifica sua política antiterror ao dispor que constitui crime inafiançável e imprescritível à ação de grupos armados, civis ou militares, contra a ordem constitucional e o Estado Democrático."

Outro dispositivo legal brasileiro importante é a Lei nº 7.170/83, que puna a conduta terrorista, definindo quais seriam os crimes contra a ordem política e social e a segurança nacional. Assim:

> Nessa legislação o artigo 20 estabelece para aquele que devastar, saquear, extorquir, roubar, sequestrar, manter em cárcere privado, incendiar, depredar, provocar explosão, praticar atentado pessoal ou atos de terrorismo, por inconformismo político ou para obtenção de fundos destinados à manutenção de organizações políticas clandestinas ou subversivas, uma pena de reclusão de 3 a 10 anos, com a previsão das causas de aumento de até o

> dobro se do fato resulta lesão corporal grave e de até o triplo se resulta morte. (CALLEGARI; LIRA, 2015, p. 732).

Ademais, o repúdio ao terrorismo também pode ser encontrado Lei de Crimes Hediondos (Lei n. 8. 072/90) em seus artigos 2°, 5°, inciso V, e 8°. Interessante é a Lei nº 10.744/03 que "dispõe sobre a assunção, pela União, de responsabilidades civis perante terceiros no caso de atentados terroristas, atos de guerra ou eventos correlatos, contra aeronaves de matrícula brasileira operadas por empresas brasileiras de transporte aéreo público" (BRASIL, 2003). Essa lei tem aplicabilidade nos casos de terrorismo envolvendo aeronaves e ainda apresenta um breve conceito de terrorismo, mesmo que seja aplicado restritamente nos casos envolvendo aeronaves, em seu §4º do art. 1º: "Entende-se por ato terrorista qualquer ato de uma ou mais pessoas, sendo ou não agentes de um poder soberano, com fins políticos ou terroristas, seja a perda ou dano dele resultante acidental ou intencional." (BRASIL, 2003).

Destarte, outro dispositivo legal recente que aborda esse assunto é a Lei da Criminalidade Organizada (nº 12.850/13), que em seu art. 1º, §2, II, esclarece que os procedimentos e infrações que se encontram nela se aplicam as organizações criminosas e também: "às organizações terroristas, entendidas como aquelas voltadas para a prática dos atos de terrorismo legalmente definidos." (BRASIL, 2013). Tal definição legal foi dada pela lei nº 13.260, de 2016, que será aborda em subtópico específico para essa lei, dada sua relevância.

O Brasil ainda ratificou pelo menos 15 convenções e protocolos internacionais que tratam da questão do 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, 2014, p. 58-59).

Além dos tratados, o Conselho de Segurança, motivado pelos atentados do 11 de setembro, elaborou algumas resoluções que exigem que os Estados:

> Implementem medidas legislativas, financeiras, de inteligência e de polícia para o combate ativo do terrorismo; adotem medidas contra o terrorismo nuclear; cooperem internacionalmente na luta contra o terrorismo; combatam, previnam e criminalizem os atos de incitamento ao terrorismo e de terrorismo; criminalizem a viagem de indivíduos para o ingresso em campos de treinamento ou em grupos terroristas no exterior; adotem medidas para garantir que terroristas não tenham acesso ao território nacional; evitem a livre movimentação de terroristas dentro do país; implementem medidas de controle das fronteiras; estabeleçam medidas de verificação de documentos; não garantam status de refugiado ou asilo para pessoas envolvidas ou que apoiaram, organizaram ou facilitaram atos terroristas. (LASMAR, 2014, p. 59).

Não obstante todo o material legislativo demonstrado acima, uma legislação definida, como lembra Lasmar (2014), é uma condição importante para qualquer modelo anti e contra terrorista, pois, esses instrumentos legais se tornam inócuos, como aponta Alcântara (2015, p. 86), "uma vez que ferem tanto o princípio da objetividade jurídica (a qual exige definição clara e precisa das ações constituidoras dos tipos penais) quanto o princípio constitucional da reserva legal (o que atesta que não há crime sem que haja lei anterior que o defina)." Além disso, precisa-se de meios investigativos que auxiliam na prevenção, necessitando um repensar da atual prática de alguns institutos do direito penal como:

> O uso de informantes criminosos e cúmplices; delação premiada; imunidade e leniência; proteção à testemunha; obstrução da justiça diante da intimidação de testemunhas, oficiais ou comunidades vulneráveis; investigações transfronteiriças; independência de promotores; facilitação do uso de equipamento técnico e de interceptação; desburocratização de investigações conjuntas; interrogatórios à distância (por vídeo ou telefone por exemplo). (LASMAR, 2014, p. 56).

Nesse sentido, Brandão e Brito (2014) ao analisar a lei de interceptação telefônica (lei n. 9.296/96 e 10.217/01) e a lei sobre infiltração policial (lei n. 12.850/13) constatam que a legislação foi construída para apurar um delito em andamento, tendo pouco efeito na prevenção de um atentado que não ocorreu, já que em relação a lei de interceptação telefônica teria a discussão sobre a legalidade de interceptação de outras formas de comunicação, como por exemplo a telemática e informática, e restaria excluída a hipótese de interceptação para assessoramento. (BRANDÃO; BRITO, 2014, p.179). Enquanto a lei sobre infiltração policial,

além de só poder ocorrer quando esgotadas todos os recursos disponíveis, ela exclui a regulamentação da infiltração de oficiais de inteligência. (BRANDÃO; BRITO, 2014, p.181).

Logo, um instrumento jurídico seria necessário, pois além da tipificação, ajudaria as atividades da agencias de inteligências brasileiras e na prevenção e combate de potenciais atentados. (LASMAR, 2014).

Porém, segundo o Lasmar (2014, p. 56), "não há dúvidas de que qualquer legislação de prevenção e combate ao terrorismo é complexa, possui um alto custo social e institucional de implementação." Por isso, as especificidades que o terrorismo apresenta trás entraves para o nosso sistema criminal 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).

Coadunamos com tal pensamento de Lasmar no que diz respeito ao ciberterrorismo, pois conforme demonstrado neste trabalho, o ciberterrorismo, além de ter um *Modus Operandi* diferente do terrorismo, atua em um ambiente diverso, que é o ciberespaço. Assim, a sua desterritorialização, em face da interação *on-line* em tempo real, bem como a rapidez com que a tecnologia se aperfeiçoa, e levando em conta a cibernética de segunda ordem, que trabalha com questões do ideal da complexidade e da noção de pensamento sistêmico, compreende-se um sistema social de interação complexa aberta, sem predeterminações. O que implica, conforme explica Renata Barros (2015, p.41), que "uma ação pode causar uma grande reação, nas relações interconectadas pelo mundo virtual da sociedade contemporânea internacional."

Além disso, como foi demonstrado nos tópicos sobre o ciberterrorismo, vimos que esse tipo de conduta não possui um conceito fechado e pode ocorrer de várias formas, o que evidencia a necessidade de construção de um sistema penal que vá além de punir, mas também trabalhe na ótica de prevenção. Logo, mais do que uma tipificação dessa conduta precisa-se de meios investigativos e processuais específicos para a proteção devida da ordem pública. Nesse sentido:

> É nesse cenário que a Ciência Criminal atua como instrumento a serviço do Direito Penal, fundamentando as razões para a criação de um controle jurídico repressivo: os tipos penais. Nesse processo, o legislador, ao interpretar os fenômenos sociais, termina por se valer da lei penal, como a primeira – ou até mesmo a única – ferramenta de controle social. (CALLEGARI; LIRA, 2015, p. 712).

Para nossa sorte a Lei Antiterrorismo (nº 13.260/2016) seguiu a tendência de vários ordenamentos jurídico de diversos países, que com base no modelo de prevenção adotado pelos Estados Unidos, pretendem aperfeiçoar essa demanda típica para uma devida atuação do Direito Penal (MENEZES, 2012). Desse modo, essa lei representou um avanço extraordinário no ordenamento jurídico brasileiro sobre o assunto, e por isso, será estudada num subtópico específico adiante.

Entretanto, há autores que são contra essa elaboração de uma legislação específica e argumentam que esse silêncio não seria um problema, já que domesticamente um ataque terrorista configuraria um ou mais crimes já existentes no direito penal pátrio. (LASMAR, 2014).

Assim, para tais autores, imaginamos que o ciberterrorismo teria solução em um concurso formal heterogêneo entre o crime de dano qualificado, art. 163 do Código Penal, com o art. 154 -A do Código Penal, que tipifica crime invadir dispositivo informático alheio mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo. O que culminaria em uma pena pífia perto do tamanho desastre causado por um atentado desse tipo.

Fica evidente a necessidade de um instrumento legislativo que aborde o ciberterrorismo de forma adequada, mesmo com os avanços da Lei Antiterrorismo (nº 13.260/2016). Para tanto, primeiramente veremos diversos projetos de lei que existem sobre o terrorismo, para demonstrar o interesse e as intenções do legislador em regularizar essas condutas diante do Direito Penal. Posteriormente, iremos analisar brevemente o que seria o emergencialismo penal, já que as legislações que abordam terrorismo tendem a ter características de um direito penal de emergência. Por fim iremos analisar a Lei Antiterrorismo (nº 13.260/2016).

## 6.1. Projetos de lei

O Brasil esta tentando se alinhar à política criminal antiterrorista da Organização dos Estados Americanos e da Organização das Nações Unidas, submetendo ao Congresso Nacional algumas propostas que visam à criação de tipos penais específicos para a criminalização do terrorismo e suas versões. Assim, neste subtópico iremos demonstrar alguma dessas tentativas.

> É importante mencionarmos que, até o momento em que esse artigo foi escrito, existem diversos projetos de lei sobre a matéria no Congresso Nacional. Entre eles, podemos citar: o projeto de lei visando negar vistos para pessoas ligadas ao terrorismo (introduzido em 2011); o projeto para a definição de terrorismo na Constituição (introduzido em 2013); o projeto de reforma do código penal que inclui em sua parte ligada aos crimes internacionais a tipificação de atos de terrorismo (introduzida em 2012); o projeto para definição e combate ao terrorismo durante a Copa do Mundo (introduzida 2011); e o projeto de emenda da Lei Federal n. 9 613/1998 para criminalizar o financiamento de terrorismo. Não obstante, como pode ser observado pelas datas em que os projetos de lei foram introduzidos, há uma grande demora em suas promulgações. Os Estados Unidos, por exemplo, são explícitos em considerarem o fato de a legislação de antiterrorismo e anti-lavagem de dinheiro estarem prontas mas não votadas como sendo a principal falha do contraterrorismo brasileiro e um reflexo da falta de vontade política em se aprovar esse tipo de lei. (LASMAR, 2014, p. 61).

Nesse sentido, temos o Projeto de Lei do Senado nº 236, de 2012, e suas proposições anexadas, de autoria do Senador José Sarney, que visa reformar o Código Penal Brasileiro. Tal projeto se encontra na Comissão de Constituição, Justiça e Cidadania (CCJ), aguardando designação do relator e se encontra parado desde 17 de julho de 2016. Tal projeto propõe:

> Incluir o crime de terrorismo, matéria que vem sendo objeto de apreciação a partir do PLS nº 707 e do PLS nº 762, ambos de 2011. A primeira inovação é a inserção do terrorismo como crime hediondo, previsão essa constante do inciso XI do artigo 56 do referido Projeto de Lei. Depois, no título dos crimes contra a paz pública, o artigo 239 trata diretamente do crime de terrorismo, o artigo 240 penaliza o financiamento do terrorismo, o artigo 241 criminaliza o favorecimento pessoal ao terrorismo e o artigo 242 prevê a majorante da metade da pena dos referidos crimes quando forem praticados durante grandes eventos. (CALLEGARI; LIRA, 2015, p. 733 - 734).

O Projeto de Lei do Senado nº 499/13, de autoria da Comissão Mista, tem escopo de consolidar a legislação federal e a regulamentar dispositivo da Constituição Federal, definindo crimes de terrorismo e estabelecendo a competência da Justiça Federal para o seu processamento e julgamento. Desse modo, esse projeto de lei tem objetivo de revogar o artigo 2º da Lei nº 7.170/83. Entretanto, tal projeto teve parecer desfavorável da Comissão de Direitos Humanos e Legislação Participativa, do Senado Federal:

> De acordo com os Senadores dessa Comissão, "da maneira como apresentado, o projeto de lei prevê tipos penais demasiadamente abertos, com penas extremamente elevadas, ofensivas aos princípios basilares de proteção aos direitos humanos". Além disso, os Senadores notaram uma desproporção em relação ao preceito secundário do tipo, já que, da forma pretendida "o tipo penal básico de terrorismo, previsto no art. 2°, prevê pena mínima de 15 (quinze) anos de reclusão, reprimenda muito superior ao tipo penal de homicídio do art. 121 do Código Penal (Decreto-Lei n°2.848, de 1940)". Conforme os integrantes da CDHLP do Senado, "a falta de proporcionalidade é evidente" se comparada à pena de homicídio, que tem previsão de seis a vinte anos de reclusão. O parecer, por fim, conclui que a

> proposta do tipo penal inserido no PLS nº 236/2012 traz uma melhor tipificação e corrige os vícios trazidos elo PLS nº 499/2013. (CALLEGARI; LIRA, 2015, p. 736).

Dessa forma, o Projeto de Lei nº 2.016/15, como lembra Callegari e Lira (2015, p. 737) foi de cunho do "Poder Executivo Federal, por meio dos Ministérios da Justiça (Min. José Eduardo Martins Cardozo) e da Fazenda (Min. Joaquim Vieira Ferreira Levy)", e visava tipificar o terrorismo na Lei nº 12.850/13 e regulamentar o disposto no inciso XLIII do art. 5º da Constituição Federal foi transformado na Lei Ordinária 13.260/16, que é a Lei Antiterrorismo, que será abordada no subtópico posterior.

Existem outras tantas propostas para tipificar o crime de terrorismo, como o PL nº 4.674/2012, de autoria do deputado federal Walter Feldman (PSDB). Tal projeto de lei além de prever a criminalização de atos de terrorismo, considera a hipótese de "narcoterrorismo", que seria as ações promovidas por facções criminosas organizadas a partir do interior dos presídios brasileiros. Já PLS nº 762/2011, de autoria do Senador Aloysio Nunes Ferreira (PSDB), pretende definir crimes de terrorismo de modo que seja tipificado a conduta de provocar ou infundir terror ou pânico generalizado mediante ofensa à integridade física ou privação da liberdade de pessoa, por motivo ideológico, religioso, político ou de preconceito racial, étnico, homofóbico ou xenófobo. Dispõe ainda que o condenado pelos crimes de terrorismo iniciarão o cumprimento da penal em regime fechado e que os crimes são inafiançáveis e insuscetíveis de graça, anistia, indulto e fiança, estabelecendo a competência para julgar os crimes de terrorismo é da Justiça Federal. Ademais, pretende revogar a Lei nº 7.170/83 que cuida dos crimes contra a segurança nacional, a ordem política e social, já acima anteriormente neste trabalho.

Ao comparar os projetos de lei nº 236/2012 (Novo Código Penal), nº 499/2013 (alteração da Lei nº 7.170/83) e nº 2.016/2015, Callegari e Lira e concluem que:

> Verifica-se que, tanto no Projeto do Novo Código Penal quanto no Projeto do Poder Executivo, o delito de terrorismo encontra uma tipificação adequada, com penas razoáveis e, embora haja algumas sinalizações de um Direito Penal expansivo, com condutas nucleares plurais e alternativas e punição a atos preparatórios e de perigo abstrato, há melhor racionalidade legislativa do que na proposta inserida pelo Projeto de Lei nº 499/2013. Dessa forma, o Brasil demonstra uma clara adesão à política criminal antiterror mundial e aos objetivos da Convenção Interamericana contra o Terrorismo, pela qual a Organização dos Estados Americanos (OEA) recomenda aos países membros a prevenção, a sanção e a eliminação do terrorismo, tudo com o compromisso de adoção de medidas necessárias e fortalecer a cooperação entre si. (CALLEGARI; LIRA, 2015, p. 738 - 739).

No que tange ao ciberterrorismo, vê-se como bem esclarece Callegari e Lira (2015, p. 739), “a partir da evolução das relações sociais e do surgimento de novos riscos, como é o caso dos atos terroristas, é possível concordar que o atual panorama da racionalidade legislativa do Brasil justifique a alteração do sistema penal vigente para produção de norma penal específica antiterror.”

Assim nesses projetos listados acima, nenhum aborda o ciberterrorismo de forma separada. No entanto, o Projeto de Lei nº 2.016/15, que virou a Lei Antiterrorismo, pelo menos trás alguma possibilidade de enquadrar a conduta em um tipo. Contudo, antes de abordar essa lei propriamente dita, se faz necessário entender a lógica emergencialista que permeia suas normas.

## 6.2. Direito Penal De Emergência

Após as análises de algumas leis brasileiras e a análise de projetos de lei que abordam a temática de terrorismo, feitas acima, ficou evidente a características de elementos de um Direito Penal de Emergência. Assim, partiremos aqui para o estudo breve do emergencialismo penal, apontando seu conceito, características e objetivos.

A volta da discussão a respeito da necessidade de um Direito Penal de exceção se deu por Jakobs com a observação das situações de mudança legislativa vivenciada na Europa na década de 80, trazido por ele através do debate sobre o denominado Direito Penal do Inimigo. (TEIXEIRA, 2017). Tal sistema faz uso da urgência e da relativização de direitos, permitindo uma aplicação legítima, mais intensa e mais imediata do poder punitivo estatal sobre aquele tal antagonista.

Nesse sentido, visa o estabelecimento de uma diferente forma de tratamento para situações específicas, consideradas de emergência, devendo, porém, assim como o direito penal “comum”, funcionar dentro do direito, ou seja, essa teoria é produto da sociedade de risco, marcada pela insegurança e pelo medo, (BONACCORSI, 2011). Essa temeridade e risco são oriundos da dinamicidade do fenômeno criminal e do desenvolvimento e ampliação da periculosidade, que são, por sua vez, advindos dos fenômenos de desenvolvimento tecnológico, globalização, ocidentalização, e da complexa trama de relações geopolíticas de um mundo marcado pelo avanço científico e pelo meio cibernético. O progresso no mundo e sua globalização intensa expandem as formas, canais e objetos da relação humana, o que, por óbvio, como consequência natural, permitem o surgimento de novos riscos e tipos de danos. Desse modo, o emergencialismo é um modelo menos garantista, com postura mais expansiva das medidas penais, tendo enfoque intervencionista e preventivo (BONACCORSI, 2011).

Esse direito penal emergencialista tem perfil não somente punitivo, mas também preventivo, com a extensão dos poderes investigativos e a adoção de medidas penais preventivas e antecipatórias diversas, partindo das maiores possibilidades de detenção até sistemas de interrogatórios mais austeros.

Além disso, tem-se que tal modelo adota a natureza de um direito penal de terceira velocidade, termo inicialmente empregado por Silva Sanchez, indicando um sistema jurídico criminal com grau de poder punitivo mais elevado e uma relativização das garantias materiais e processuais, retirando parte das restrições a atuação penal do Estado (SANTOS, 2012).

Entretanto o que se abrange ao dizer situações de emergência? Trata-se de momentos de instabilidade, onde se põe em risco, bem como em xeque, os direitos fundamentais humanos, devem eles serem respeitados em toda e qualquer situação?

A partir disto, dividem-se as situações de emergências em três categorias: natural, quando estiver abordando situações de crise decorrentes de fenômenos naturais; tecnológica, no que tange instalações e infraestrutura e problemas no seu funcionamento; por fim, situações de emergência complexa, onde há grande violência, colocando-se em risco a vida de pessoas devido a fatores políticos e a própria comunidade. (TEIXEIRA, 2017). Contudo, há de se observar que os conceitos apresentados são abstratos, mas que permitem a realização de verificações de sua ocorrência caso a caso.

Pensa-se também desta maneira a respeito de classificação das situações de emergências a partir de níveis, sendo as de posições mais baixas as situações que podem ser tratadas pelos sistemas vigentes e as de níveis mais alto quando se torna necessário agir fora do direito, a partir de decisões políticas, já que o primeiro não possui meios de combate a este. Assim, segundo Teixeira (2017, p.135), “a consequência da ideia de exceção como algo para além do direito é a afirmação da maior amplitude da Política em relação ao Direito, de forma que devem existir atos políticos que não podem ser limitados pelo sistema jurídico.” Apesar disto, os atos políticos devem obedecer, ou ter a aparência de que respeitam determinados limites de um Estado Democrático de Direito.

A partir desta situação, volta-se a supramencionada teoria do Direito Penal do Inimigo, importante ressaltar que em tal concepção, o chamado inimigo não precisa, necessariamente, agir a partir de motivações políticas, tal qual ressaltado no conceito de emergência complexa, mas, torna-se inimigo apenas as pessoas que assim o querem, passando a serem considerados como “não-pessoas”, neste sentido:

> *Não-pessoa* é quem não oferece segurança cognitiva sobre seu próprio comportamento ser fiel ao Direito ou não, por se recusar a assumir os

> deveres e direitos que a ideia de pessoa demanda. Assim, não é propriamente o Direito que exclui ou subtrai de determinadas categorias de indivíduos a qualidade de ser pessoa (...), mas são estes próprios que se auto excluem a partir do momento em que não agem como tal, a partir do momento em que não oferecem mais garantias a respeito das expectativas de conduta social que sobre eles recaem. Por essa razão, ou seja, por ser uma auto exclusão, é que logo no início do desenvolvimento de sua teoria Jakobs afirma que é preciso manter em aberto a possibilidade do *indivíduo* voltar à condição de cidadão de *pessoa*. Afinal, a autonomia dele enquanto ser humano deve ser garantida, sob pena de se descaracterizar o Estado de direito. (TEIXEIRA, 2017, p.238). (grifos do autor).

Inúmeras foram as críticas recebidas por tal teoria, dentre elas a falta do conceito de dignidade humana, bem como a instituição, política, de quem seria este inimigo. Critica-se, também, o fato de se levar em consideração um único sistema, e a partir dele e sua cultura, considerar quem seria o inimigo, mesmo que o conceito de "pessoa" seja apenas jurídico, ou seja, livre de preconceitos culturais, históricos, étnicos.

A partir do exposto, resta deixar claro a necessidade de um Estado de Direito já consolidado, para que não haja risco de sua falência com a atuação de um Direito Penal de Emergência, pois conforme explica Teixeira (2017, p. 260), "a elaboração de Direito de Emergência só se legitima se mostra apta à contribuir para a consolidação do Estado de direito contemporâneo, com todas as implicações que o conceito tem hoje."

Por fim, enfatiza-se a necessidade de se respeitar os direitos fundamentais humanos, e que o Direito Penal de Emergência tenha como base certos direitos básicos e trabalhe, então, a partir deste limite realizar sua atuação, tais como a liberdade de escolha, de manifestação e a presunção de inocência. (TEIXEIRA, 2017). Este deve ser sempre o guia do Direito Penal, seja ele o "comum" ou o de exceção, abordado no presente tópico.

## 6.3. Medidas típicas de um direito penal de emergência no ciberterrorismo

Nesse contexto, onde o ciberterrorismo, através de ataques que objetivam o medo e pânico em toda a população, tem o intuito de intimidar ou coagir governos ou sociedades em busca de objetivos políticos, religiosos ou ideológicos, é razoável entender que o ciberterrorista, assim como o terrorista convencional, poderia ter um tratamento típico de um direito penal de emergência. Assim, deve-se constatar que:

> 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, 2017)

Dessa forma, a criação de um sistema específico para o ciberterrorismo seria interessante, pois, o Estado atuaria no mesmo plano dos atores do ciberterrorismo, visto que o ambiente do ciberespaço é distinto do convencional e compreende o ideal de complexidade. Podendo assim, aumentar suas chances de sucesso na efetiva prevenção e punição desta conduta.

Estando então compreendidos a parte teórica do direito penal de emergência, que influencia na elaboração de leis antiterroristas, e sua relação com o ciberterrorismo, passamos para análise da Lei Antiterrorismo que tenta normatizar tais situações.

## 6.4. Lei Antiterrorismo (13.260/2016)

O Brasil ao tentar se alinhar à política criminal antiterrorista do restante do mundo criou o projeto de lei nº 2.016/15, que visava de algum modo tipificar os atos terroristas, para que caso houvesse algum incidente nas Olimpíadas de 2016, realizada no Rio de Janeiro, tal atentado não passasse impune, cuja pena prevista é "reclusão, de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência" (BRASIL, 2016). Ademais, tal lei visa evitar o que já aconteceu no passado no:

> Ato terrorista do grupo palestino Setembro Negro, o qual sequestrou atletas israelenses nos Jogos Olímpicos de Munique de 1972, tendo como resultado a morte de onze dos atletas israelenses, cinco dos terroristas palestinos e um policial alemão, devido à ausência de planos de prevenção e de um grupo especializado para tais situações. (JÚNIOR, 2016, p.2).

Além disso, é relevante se atentar para o fato de que

> O governo brasileiro, desde 2010, havia se comprometido perante o GAFI (Grupo de Ação Financeira contra Lavagem de Dinheiro e o Financiamento do Terrorismo) a elaborar uma norma jurídica acerca do referido assunto, que contivesse punições específicas para o financiamento do terrorismo. A ausência desta legislação resultaria na desabonação do Brasil como um bom país para se investir. (ABREU, 2016).

E é nesse contexto que temos a criação da Lei 13.260/16, que entrou em vigor em 18 de março de 2016 e regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, buscando disciplinar o terrorismo, criando o tipo penal do terrorismo. Além disso, essa lei ira tratar de disposições investigatórias e processuais e o julgamento de tal crime. Desse modo, como lembra Vladimir Júnior (2016, p.7), "ainda, prevê os crimes ligados a essa prática

(organização terrorista, financiamento, treinamento,...), além de explicitar quando não é aplicável a manifestações públicas.

A Lei Antiterrorismo em seu art. 2º define o conceito de terrorismo:

> 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. (BRASIL, 2016).

Ao usar as expressões "por razões de"; "quando cometidos com a finalidade de", esse tipo exige uma conduta com um dolo específico. Assim, partindo do dolo específico deste artigo, nos parágrafos seguintes a lei busca delinear o que seria atos de terrorismo. Dessa forma, segundo Vladimir Júnior (2016, p.8), "para evitar a má aplicação dos tipos penais ou que eles sejam vagos, devemos analisar a conduta tipificada e somar ao *caput* do artigo 2º, o qual dispõe o dolo específico de todos os crimes."

Em outras palavras, a definição legal de terrorismo está estruturada da seguinte forma:

> 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. (GOMES, 2016).

Para nosso trabalho, relevante é o §1º, inciso VI deste artigo, que 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; (BRASIL, 2016).

Desse modo, esse é melhor enquadramento para a conduta de ciberterrorismo no atual ordenamento jurídico brasileiro. Assim, as condutas

> "Sabotar" (prejudicar; impedir funcionamento) ou "apoderar-se" (tomar posse; apoderar-se), na primeira parte usando-se da violência ou da grave ameaça à pessoa e na segunda utilizando de mecanismos cibernéticos (mecanismos de controle e comunicação de máquinas), o controle estruturas fundamentais para a sociedade, como comunicação, transporte, hospitais, instituições de controle e armazenamento de água e energia. (JÚNIOR, 2016, p.9).

Se não vejamos, ao conjugar essas condutas com o dolo específico do *caput* do art. 2º [22], com por meio de mecanismos cibernéticos, sabotar ou apoderar com violência ou grave ameaça, o controle de estruturas fundamentais, como o rol exemplificativo do dispositivo[23], temos uma definição próxima dos conceitos de ciberterrorismo, já discutidos neste trabalho, pois, o ciberterrorismo tem o intuito de intimidar ou coagir governos ou sociedades em busca de objetivos políticos, religiosos ou ideológicos. Nesse sentido é precisa a análise:

> O art. 2º, §1º, inc. IV da Lei Antiterrorismo tipifica penalmente a conduta do agente (qualquer pessoa, só ou em colaboração com outrem, haja vista ser crime comum e de concurso eventual) que sabotar (impedir ou perturbar) o funcionamento ou apoderar-se (tomar posse), com violência, grave ameaça à pessoa ou servindo-se de mecanismos cibernéticos (meios de execução), 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, desde que presente as razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, e com o fim de provocar (o metafísico, e, portanto, criticável) terror social ou generalizado, de forma a expor a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública (trata-se de crime de perigo comum, que expõe a risco um número indeterminado de pessoas). Desse modo, motivos políticos ou econômicos, por exemplo, descolados desses requisitos, não conduzem à configuração do crime em comento. Trata-se, portanto, de tipo misto alternativo, sendo cabível a tentativa, dado sua natureza plurissubsistente. Inobstante, é crime comissivo, formal, de perigo concreto, pluriofensivo e de dupla subjetividade passiva. (ALMEIDA; CUNHA, 2017).

Nesse ínterim, os autores acima fazem uma análise acerca da possibilidade de enquadramento de ciberterrorismo, previsto na lei de antiterrorismo, ataque cibernético do dia 12 de maio de 2017 pelo vírus (*malware*) *WanaCrypt0r*, que é uma variação do vírus

---

[22] "Quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública." (BRASIL, 2016)

[23] "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;" (BRASIL, 2016)

*WCry/WannaCry*, explicado os acontecimentos mais detalhados no tópico de ciberterrorismo deste trabalho, e concluem tal enquadramento não seria possível:

> Embora o(s) agente(s) tenha(m) sabotado o funcionamento de um dos entes listados (ex: hospitais, estações ferroviárias), servindo-se de mecanismos cibernéticos enquanto meio de execução, de modo a expor a perigo patrimônio, a paz pública ou a incolumidade pública, as razões exigidas no tipo penal (de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião) não estão presentes. Em relação ao terror social ou generalizado, não se pode afirmar que o(s) agente(s) o tenha(m) perseguido, ainda que, no plano concreto, a depender da interpretação, possa tê-lo causado (e não importa causá-lo, mas sim ter a intenção de causá-lo). Outrossim, a exigência de resgate denota que o(s) autor(es) buscava(m) obter vantagem econômica, o que afasta, *prima facie*, o dolo de ciberterrorismo, eis que este tipo penal não perquire tal fim. Neste compasso, possível desconfiança de que a exigência de resgate tenha visado o financiamento do terrorismo ou, então, disfarçado o intento de busca de informações sensíveis que sejam válidas para futuras ações terroristas está, por ora, tão somente no campo da mera suposição. Diante do exposto, conclui-se que o ciberataque do dia 12 de maio de 2017 mais se assemelha ao crime de extorsão (art. 158 *caput* do Código Penal), ou mais propriamente à ciberextorsão, posto ter sido executado pela internet. A ciberextorsão foi, *in casu*, caracterizada pelo fito do agente em obter vantagem econômica indevida para si ou para outrem, mediante o constrangimento à vítima para que esta faça o pagamento de resgate para liberação de acesso a seus arquivos informáticos bloqueados, sob a grave ameaça de destruição de tais arquivos. (ALMEIDA; CUNHA, 2017).

Isto posto, a pena também para ser adequada para a gravidade do atentado que pode possuir danos imensuráveis. Desse modo, a pena é de reclusão, de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência. Ou seja, além da pena de 12 a 30 anos de reclusão, o sujeito, como lembra Vladimir Júnior (2016, p.9) “ainda irá responder pela pena do crime correspondente a ameaça (ameaça, porte ilegal de arma de fogo ou de explosivo ou incendiário,...) e do crime correspondente à violência (lesão corporal ou homicídio).” Em vista disso:

> Por um raciocínio lógico-jurídico, entende-se que aqui se impõe o concurso formal impróprio, do artigo 70, segunda parte, do Código Penal, o qual segue a regra do concurso material, somando-se a pena do crime de Terrorismo com a de cada crime correspondente à ameaça ou à violência, se o agente teve a intenção de ofender mais de um bem jurídico com desígnios autônomos, ou seja, desejando os vários resultados. (JÚNIOR, 2016, p.9).

Destarte, esta lei em seu art. 5º criminaliza a conduta de realizar atos preparatórios, que seria uma parte do caminho do crime antes da execução ou, melhor dizendo, do *iter criminis*, nos seguintes termos: “Realizar atos preparatórios de terrorismo com o propósito inequívoco de consumar tal delito: Pena - a correspondente ao delito consumado, diminuída de um quarto até a metade.” (BRASIL, 2016).

Contudo, pode haver discussão no sentido de que não se pode punir a cogitação e a preparação, já que o agente poderia desistir do ato criminoso a qualquer instante. Entretanto, nesta ocasião temos um tipo penal próprio para os atos da fase preparatória de um ato terrorista. Nesse sentido:

> Como exemplo de aplicação deste artigo, imaginemos que Tício ligue para Caio dizendo que explodirá um trem do metrô no dia seguinte e que está tudo preparado, sendo que tal ligação foi legalmente interceptada e que a polícia, na manhã seguinte e com o devido mandado judicial, ingressa na casa de Tício e encontra documentos sobre o plano e os explosivos. Não se deve aguardar o início da execução de crimes tão graves para punir agentes terroristas e foi exatamente o que este dispositivo buscou fazer: punir a preparação inequívoca de ato terrorista.A pena,por óbvio, é menor do que a do crime consumado, subtraindo-se de ¼ a ½ da pena daquele. (JÚNIOR, 2016, p.13).

Colaborando com a discussão, tem que se ressaltar que:

> Certamente surgirão correntes doutrinárias criticando a criminalização dos atos preparatórios aqui expostos, sob a alegação de que estaria sendo violado o princípio da ofensividade, inerente ao direito penal, assim como poderia se estar priorizando o Direito Penal do autor em face ao Direito Penal do fato. Sem discordar da possibilidade de opiniões contrárias, parece que a tipificação de atos preparatórios de terrorismo mostra-se adequada e proporcional, tendo em vista a necessidade de um direito penal, ao menos, de terceira velocidade em contraponto a tais condutas que, não raras vezes, assolam toda a humanidade. Ainda mais em momento de proximidade de evento mundial a ser recebido pelo Brasil. (AMARAL, 2017).

Nesse sentido, não há como negar que existem determinadas condutas, principalmente as que caracterizam crimes de perigo, que merecem atenção especial e mecanismos para que sejam, ao máximo evitadas, como, ao que parece, a de terrorismo, e no nosso caso, o ciberterrorismo, já que analogicamente a esta tipificação de ato preparatório terrorista, a descoberta de um ataque deste tipo, que tem proporções e gravidades gigantescas, justificaria a punição de ato preparatório e efetiva prevenção.

Contribuindo com a discussão Henrique Hoffmann Monteiro de Castro e Adriano Sousa Costaaso esclarecem sobre como ocorrem, na lei de antiterrorismo, a punibilidade antecipada da tentativa, da desistência voluntária e do arrependimento eficaz. Assim se

> O agente pratique atos preparatórios imediatamente anteriores ao verbo nuclear do terrorismo, e não ocorrer a consumação por circunstâncias alheias à sua vontade, incide a tentativa antecipada (artigo 5º, *caput* – pena do crime consumado reduzida de 1/4 a 1/2). Já se o indivíduo abandonar voluntariamente a empreitada criminosa, ocorre a desistência voluntária ou arrependimento eficaz antecipados (artigo 10 – responde pelos atos praticados). Imagine o exemplo: o agente monta arma de fogo de uso restrito com capacidade de cinco munições (sem potencial de causar destruição em massa) para se tornar acionável por controle remoto, a fim de matar alguém em meio à multidão e causar terror social por discriminação religiosa. Se é

> impedido de acionar a arma responde pelo crime do artigo 2º, §1º, V da Lei 13.260/16 com pena diminuída (combinado com artigo 5º, *caput)*. De outro lado, se desiste de acionar o dispositivo responde pelo delito do artigo 16 da Lei 10.826/03 (desistência voluntária antecipada), e se aciona a arma mas empurra o alvo, evitando seu atingimento, responde pelos artigos 15 e 16 da Lei 10.826/03 (arrependimento eficaz antecipado). (CASTRO; COSTA, 2016).

Ademais, o art. 7º dessa lei trás uma majorante que dispõe que "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." (BRASIL, 2016). Se caso um ataque ciberterrorista vá além do terror psicológico e vier a causar vítimas, o ciberterrorista tera sua pena aumentada.

Desse modo, o sistema penal clássico mostra-se insuficiente para o combate a crimes de maior complexidade e gravidade, assim, o combate a condutas de terroristas e ciberterroristas ao escapar dos sistemas clássicos de punição, através dessa lei, talvez possa encontrar mecanismos efetivos de controle destes atos.

Esta lei ainda dispõe sobre algumas regras processuais especiais que podem ser utilizadas no ciberterrorismo. A primeira diz respeito à competência, já que em seu art.11 preconiza a lei que tais crimes serão contra o interesse da União. Logo, a competência é da Justiça Federal para processar e julgar e é atribuição da Polícia Federal investigar, nos termos do inciso IV do art.109 da Constituição Federal.

> Nestes casos, o magistrado pode, de ofício, havendo indícios suficientes de crime previsto nesta Lei, decretar, no curso da investigação ou da ação penal, medidas assecuratórias de bens, direitos ou valores do investigado ou acusado, ou existentes em nome de interpostas pessoas, que sejam instrumento, produto ou proveito de crimes ligados às práticas terroristas. (CAVALCANTI; GOMES, 2016, p. 394).

Vale mencionar que existe a possibilidade de prisão temporária nos crimes previstos na lei de terrorismo, quando houver fundadas razões, de acordo com qualquer prova admitida na legislação penal, conforme alteração na redação da Lei nº 7960/89. (CAVALCANTI; GOMES, 2016).

Por fim, em seu art. 19 a lei dispõe sobre a aplicação de medidas investigativa. Aplicando todas as medidas do art. 3º da Lei de Organizações Criminosas de 2013, vejamos análise mais detalhada de Vladimir Júnior:

> I - colaboração premiada; II - captação ambiental de sinais eletromagnéticos, ópticos ou acústicos: visa colher provas por sinais eletromagnéticos, por imagens ou por sons, necessitando de autorização Judicial; III - ação controlada (flagrante retardado/esperado): visa atrasar a intervenção policial para que a prisão seja feita em momento mais eficaz para a colheita de

> provas e para prisão do maior número de criminosos possível, devendo ser feito sob observação; IV - acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais; V - interceptação de comunicações telefônicas e telemáticas: regida pela Lei nº 9.296/96, é instrumento para adquirir provas em investigações criminais através de interceptações telefônicas e de comunicações em sistemas de informática e telemática por representação do da autoridade policial ou por requerimento do Ministério Público, sendo necessário indícios razoáveis de autoria ou de participação em infração penal, que a prova não possa ser feita por outros meios e que o fato não constitua infração penal com pena de detenção; VI - afastamento dos sigilos financeiro, bancário e fiscal: visa o acesso a dados e informações que possam levar a autoria ou participação de crimes, útil para fiscalizar o patrocínio à terroristas; VII - infiltração, por policiais, em atividade de investigação: visa inserir agentes policiais em grupos criminosos para colher provas e, se possível, evitar crimes. Necessita de Autorização Judicial que, conforme o parágrafo único do referido artigo, é estritamente sigilosa enquanto durar a medida; VIII - cooperação entre instituições e órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal. (JÚNIOR, 2016, p.17-18).

Em vista disso, temos vários meios de investigações aplicáveis ao ciberterrorismo com destaque dos incisos II e V, que referem as possibilidades de interceptação de dados, o que é seria muito útil para a prevenção deste tipo de atentado.

Contudo, é necessária a harmonização de estratégias de controle preventivo e repressivo com a sistemática constitucional do Estado Democrático de Direito, pois, tais situações de interceptações de dados afrontam a privacidade dos cidadãos, e por isso, nunca deverá ser regra, mas sim exceção, justificada pelo situação emergencial do caso concreto.

Enfim, o fato de existir uma lei federal que prevê condutas tipificadas, penas, medidas processuais e investigativas de acordo com as especificidades que o terrorismo tradicional e o ciberterrorismo apresenta, conclui-se que é evidente o avanço que esta lei trás em relação ao combate de possíveis atentados que o Brasil pode vir a sofrer. Entretanto, como lembra Vladimir Júnior (2016, p. 19), “cabendo agora aos órgãos de Segurança Pública, de Defesa e outros a ele ligados (Sistema Penitenciário, Defesa Civil, Centro de Controle de Doenças, Hospitais,...) a antecipação de ameaças e a proteção da nação.”

Em conclusão, a lei de antiterrorismo já teve sua primeira aplicabilidade em caso concreto, que foi na chamada operação *hashtag*. A ação penal Nº 5046863-67.2016.4.04.7000/PR, julgada pela Justiça Federal da Seção Judiciária do Paraná da 14ª Vara Federal de Curitiba, em uma sentença de 99 páginas, oito réus foram condenados na lei antiterrorismo em seu art. 3º que dispõe que é crime "promover, constituir, integrar ou prestar auxílio, pessoalmente ou por interposta pessoa, a organização terrorista". (BRASIL, 2016).

Todos eles já haviam sido presos preventivamente pouco antes dos Jogos Olímpicos do Rio de Janeiro de 2016. Conforme relata a notícia do G1, na denúncia feita Ministério Público Federal (MPF), os indivíduos promoviam a organização terrorista denominada Estado Islâmico. “Ainda conforme a acusação, essa promoção ocorria via redes sociais, compartilhamento de materiais extremistas e trocas de email, por exemplo.” (DIONÍSIO, Bibiana; FONSECA, Alana; GIMENES, Erick, 2017). Além disso, o indivíduo que assumiu a posição de líder do grupo foi condenado no art. 5º da referida lei por realizar atos preparatórios de terrorismo com o propósito inequívoco de consumar tal delito.

## 7. CONSIDERAÇÕES FINAIS

O ciberterrorismo é o desdobramento do terrorismo que ocorre no ciberespaço, e assim como o terrorismo tem o intuito de intimidar e coagir governos ou sociedades, através do pânico e medo, em prol de seus objetivos. Assim, para ter um entendimento sobre ciberterrorismo é necessário assimilar o terrorismo convencional, que hoje se encontra na fase de terrorismo pós moderno, onde ele se tornou global.

Desse modo, o terrorismo é um ato de quem já abriu mão de soluções políticas, e é por isso que esse ataque busca através da violência e medo alcançar os seus objetivos. Tamanha aversão por esses atentados pode ser entendido ao analisar seu *modus operandi*, que preceitua, por exemplo, que um ataque terrorista deve ser quando e onde menos se espera, devendo obter o maior número de vítimas possíveis, para que seja possível abater moralmente os inimigos e deixar a sociedade refém do pavor e medo.

Em vista disso, o ciberterrorismo vem potencializar o terrorismo convencional, uma vez que ocorre no ciberespaço: um ambiente diferente que compreende uma sistemática diferente para estes fenômenos. O ciberespaço é um ambiente virtual de comunicação e transmissão de dados, sem fronteiras e que comporta mudanças mais velozes que o mundo físico. Possui a internet como principal plataforma de acesso, contendo assim a sistemática da cibernética de segunda ordem, pois, esta trabalha com questões do ideal da complexidade, onde há uma um sistema social de interação complexa e aberta, podendo uma ação causar uma grande reação.

Dessa forma, o espaço cibernético é um ambiente que possui vulnerabilidades, sendo um ambiente perfeito para a atuação de diversas condutas ilícitas. Logo, um simples indivíduo pode ser capaz de afetar o funcionamento de hospitais e tráfego de aeronaves, como o ataque cibernético realizado no dia 12 de maio de 2017 pelo vírus (*malware*) *WanaCrypt0r*.

Nesse sentido, mesmo havendo discordância entre os pesquisadores da área, não se pode ter certeza se um ataque ciberterrorista já ocorreu. Entretanto, restou comprovado que é possível que um atentado deste tipo tenha totais condições de acontecer, visto o estudo realizado em 2007 pelo *Idaho National Laboratory*, que demonstrou como é possível destruir uma infraestrutura de um gerador de diesel, apenas com o uso de computador por hackers. Não obstante, o medo pela possibilidade que tal ataque ocorra não é exagerado, conforme estudo realizado por Michael L. Gross, Daphna Canetti e Dana R. Vashdi, que demonstram que pessoas que foram expostas a possibilidades de ataques ciberterroristas compartilharam sintomas de estresse, ansiedade, insegurança e preferência pela segurança sobre a liberdade; sendo estes traços muitos semelhantes com os que a população apresenta em relação a um atentado de terrorismo convencional.

O ciberterrorismo, assim como o terrorismo, não apresenta um consenso acerca de seu conceito, assim fica evidente a dificuldade para criar um tipo penal específico para essa conduta. O que nos leva a crer que os dogmas da legalidade e da tipicidade cerrada para esse tipo de criminalidade são insuficientes. Contudo, em termos gerais, nos parece que o ciberterrorismo é um ataque a sistemas de computadores, informações e/ou dados, cometido através de um fator tecnológico, tendo o intuito de intimidar ou coagir governos ou sociedades em busca de objetivos políticos, religiosos ou ideológicos. Além disso, esses ataques, que geralmente não possuem um padrão, devem ser potencialmente capazes de causarem e espalharem o medo e pânico em toda a população.

Apesar de ser da dificuldade em encontrar um tipo específico para essa conduta, ao analisar os objetivos, fica evidente a existência de um dolo específico que o diferencia de cibercrimes comuns. O ciberterrorismo tem objetivos simbólicos e mortíferos, já que com o intento de causar danos graves às liberdades mais simples, como poder comer, beber, mover-se e viver dos cidadãos, agindo para o governo seja coagido a realizar seus objetivos. Assim, seus alvos de preferência são aqueles que os meios de comunicação social irão dar mais enfoque, aumentando a sensação de pânico. Justamente por isso, seus alvos são programas de gestão e controle de serviços essenciais a um Estado, como, por exemplo, redes de distribuição elétrica, de água potável, bancárias e financeiras.

Os atores do ciberterrorismo são pessoas que possuem profundo conhecimento de informática, alguns inclusive com habilitações acadêmicas elevadas como Mestrados e Doutorados. Essas pessoas possuem um vasto arsenal, como por exemplo: vírus (*malware*), *worms*, *spywares*, bombas de impulso eletromagnético, munições de radiofrequência, dispositivos eletromagnéticos transitórios, *back doors, trap doors, virtual sit-ins, e-mail*

*bombs e botnets*. Sendo a criatividade humana o limite, o que permite que existam variadas formas para que um ataque ciberterrorista ocorra.

Isto posto, fica evidente a diferença entre ciberguerra, cibercrime e ciberterrorismo. Ou seja, na ciberguerra há uma agressão promovida por um Estado destinada a danificar a capacidade do outro para impor seus objetivos. Já o cibercrime, por mais que possa se confundir com o ciberterrorismo, geralmente é motivado para conseguir benefícios econômicos próprios, enquanto o ciberterrorismo possui um dolo específico de causar o maior dano possível, por razões políticas ou religiosas, fazendo com que o governo e a população se submetam a suas vontades por meio do medo.

Desse modo, devido às diversas facetas que um ataque ciberterrorista pode ter, parece ser impossível criar um tipo penal fechado para esta conduta. Talvez a maneira mais desejável de lidar com tal situação seria a construção de um tipo penal mais aberto, que tivesse algum rol exemplificativo de condutas e a previsão de um dolo específico que conduzissem a devida leitura do dispositivo, para que os aplicadores do direito através da hermenêutica penal pudessem identificar condutas, que mesmo não sendo idênticas as do rol exemplificativo, caracterizariam uma ação ciberterrorista.

Os governos mundiais estão atentos a gravidade desta matéria e já estão visando a cibersegurança cada vez mais, seja por meio de criação de órgãos específicos, implementação sistemas de vigilância até como adaptando seus ordenamentos jurídicos para essa nova realidade.

Sobre os órgãos específicos temos que o Brasil ao criar seu Centro de Defesa Cibernética (CDCiber) acompanha países como Estados Unidos, que possuem CIAO e o NIPC, China, que possui o Centro de Guerra de Informação, o Japão, que tem cerca de 30 especialistas em informática a disposição do chefe de Segurança do Governo, a Espanha, que tem o CERT, e até mesmo nossa vizinha Argentina, que possui um Escritório de Coordenação de Emergências em Redes Telemáticas.

Já em relação aos sistemas de vigilância foi apresentado o Echelon, o “Carnivore”, o “Dark Web”, o OSEMINTI e o FISC, que são sistemas que buscam antecipar as informações sobre possíveis atentados terroristas, mas abrem uma discussão sobre o limite dessas inserções na privacidade dos cidadãos e o problema acerca da retenção destes dados. Tal questão é complexa e ainda não possui uma resposta pronta. Contudo, tal interferência poderia ser justificada pela segurança pública. Parece que o campo de debate para esse assunto se encontra aberto, já é necessário encontrar um equilíbrio entre a privacidade e a segurança pública a todo custo.

Os ordenamentos jurídicos de diversos países também estão passando por adequações para essa nova realidade. O primeiro país a fazer alterações em seu ordenamento foi os Estados Unidos, motivados pelo 11 de setembro, com o *Patriot Act* que adotou uma série de medidas em relação ao combate ao terrorismo. Para o combate do ciberterrorismo importante foram as medidas de vigilância criadas por essa lei, como uma maior possibilidade de interceptação de comunicação (qualquer que seja o meio utilizado, como email e ligações telefônicas), maior compartilhamento de informação entre agências de segurança e inteligência e uma permissão que possibilita um atraso na notificação de mandados de *"sneak and peak"*, ou seja, desde que seja aparente a possibilidade de ataque cibernético, o computador de um ciberterrorista poderia ser invadido e vasculhado.

Nesse sentido, países como a Suécia, Reino Unido e Grécia também possuem legislações severas para coibir e punir ações características de ciberterrorismo. Já recentemente a França, após sofrer uma série de atentados terrorista em seu território, sancionou a nova lei antiterrorismo que visa que as forças de segurança ganhem mais poder para conseguir realizar buscas e apreensões e restringir a movimentação de suspeitos de ligação com organizações terroristas.

O Brasil em sua Constituição de 1988 em seus artigos 4º, VIII e 5º, XLIII, já expõem o repúdio ao terrorismo, sendo este considerado um crime hediondo, sem possibilidade de fiança, anistia ou indulto. Ademais, a Lei nº 7.170/83, já punia a conduta terrorista. Tal questão é abordada na Lei nº 8.072/90, Lei nº 10.744/03 e na Lei nº 12.850/13. O Brasil no cenário internacional é claro ao se colocar contra o terrorismo ao ratificar pelo menos 15 convenções e protocolos que tratam da questão de combate ao terrorismo.

Entretanto, uma legislação específica é necessária, pois, ela deve ir além da tipificação da conduta, devendo abordar meios investigativos e processuais adequados para esse assunto. Tal lógica também é verídica em relação ao ciberterrorismo, já que atua em um ambiente diverso ao terrorismo convencional, que aplica em um desterritorialização e maior agilidade de mutação, conforme o desenvolvimento da tecnologia e maior dependência das sociedades de redes eletrônicas.

O legislador brasileiro buscando aprimorar seu ordenamento, em relação às disposições constitucionais e alinhar à política criminal antiterrorista da ONU, submeteu ao Congresso Nacional alguns projetos de lei (PL) como o PL do Senado nº 236/12, o PL nº 499/13, o PL nº 4.674/12, o PL nº 762/11 e o PL nº 2.016/15 que se tornou a Lei Ordinária 13.260/16, que é a Lei Antiterrorismo.

Não obstante, tais projetos de lei e a Lei Antiterrorismo têm caráter de um Direito Penal de Emergência, que é uma teoria que é produto da sociedade de risco, que tem como características a insegurança e o medo. Assim, faz uso da urgência e da relativização de direitos, permitindo uma aplicação legítima, mais intensa e mais imediata do poder punitivo estatal. Esse direito penal emergencialista tem perfil não somente punitivo, mas também preventivo, com a extensão dos poderes investigativos e a adoção de medidas penais preventivas e antecipatórias diversas, partindo das maiores possibilidades de detenção até sistemas de interrogatórios mais austeros.

Nesse contexto, e depois de toda a análise realizada acerca do ciberterrorismo e do ambiente onde ele ocorre, o ciberespaço, é razoável entender que o ciberterrorista, assim como o terrorista convencional, poderia ter um tratamento típico de um direito penal de emergência, visto que a criação de um sistema específico para essa conduta poderia ser mais adequado para sua efetiva prevenção e punição, já que os instrumentos tradicionais de controle se tornaram inócuos no combate deste crime.

Por fim, em 2016 o legislador brasileiro enfim aprovou a Lei Antiterrorismo, regulamentando as normas constitucionais do inciso XLIII do art. 5º, buscando disciplinar o terrorismo, criando um tipo penal, e prevendo disposições investigatórias e processuais de tal crime. Apesar de não ter regulado de maneira completa o ciberterrorismo, é louvável o avanço que essa lei apresenta. Em seu art. 2º, §1º, inciso VI, que é o melhor enquadramento existente para a conduta de ciberterrorismo no atual ordenamento jurídico brasileiro.

Para tanto, o dolo específico, que é finalidade de provocar terror social ou generalizado, conjugado com “por meio de mecanismos cibernéticos, sabotar ou apoderar com violência ou grave ameaça, o controle de estruturas fundamentais”, como o rol exemplificativo do dispositivo, temos uma definição próxima dos conceitos de ciberterrorismo, já discutidos neste trabalho, pois, o ciberterrorismo tem o intuito de intimidar ou coagir governos ou sociedades em busca de objetivos políticos, religiosos ou ideológicos.

Enfim, o fato de existir uma lei federal que prevê condutas tipificadas, penas, medidas processuais e investigativas de acordo com as especificidades que o terrorismo tradicional e o ciberterrorismo apresentam, conclui-se que é evidente o avanço que esta lei traz em relação ao combate de possíveis atentados que o Brasil pode vir a sofrer. Entretanto, ressaltam-se a necessidade de uma lei específica que crie um sistema para o crime de ciberterrorismo e demais crimes virtuais, já que lógica do ciberespaço altera a dinâmica linear baseada na ideia de causa e efeito do direito penal convencional.

## REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Karina Medeiros de. **Considerações sobre o crime de terrorismo nos cenários nacional e internacional e breves apontamentos acerca da Lei 13.260 de 17/03/2016 - Antiterrorismo.** Conteudo Juridico, Brasilia-DF: 19 abr. 2016. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=2.55677&seo=1>. Acesso em: 23 nov. 2017.

AGUILAR, Sérgio Luiz Cruz. **Os esforços da sociedade internacional no combate ao terrorismo.** Em 3° Encontro Nacional, São Paulo, 2011. Disponível em: <http://www.proceedings.scielo.br/scielo.php?script=sci_arttext&pid=MSC0000000122011000300046&lng=en&nrm=iso>. Acesso em: 28 jul. 2017.

ALCÂNTARA, Bruna Toso. **Brasil e Ciberterrorismo: desafios para o Rio 2016.** The Ninth International Conference On Forensic Computer Science - ICoFCS 2015. Disponível em: < http://icofcs.org/2015/ICoFCS-2015-011.pdf>. Acesso em: 14 nov. 2017.

ALMEIDA, Débora de Souza de; CUNHA, Rogério Sanches. **O ciberataque do dia 12 de maio: ciberterrorismo?** Meusitejurídico.com. Pub. 16 de maio de 2017. Disponível em: <https://pdfdocumento.com/ciberterrorismo-amazon-simple-storage-service-s3_59cb63161723dd07b65c80cd.html>. Acesso em: 23 nov. 2017.

AMARAL, Vinicius Pascueto. **Lei 13.260/2016 "Antiterrorismo" - A tipificação de atos preparatórios.** Jusbrasil. Disponível em: < https://pascuetoamaral.jusbrasil.com.br/artigos/317284328/lei-13260-2016-antiterrorismo-a-tipificacao-de-atos-preparatorios>. Acesso em: 28 jul. 2017.

BARROS, Renata Furtado de. **Guerra Cibernética: Os Novos Desafios do Direito Internacional.** Belo Horizonte: Editora D'Plácido, 2015.

BATISTA, Gonçalo; RIBEIRO, Carlos; AMARAL, Feliciano. **Ciberterrorismo: a nova forma de crime do séc. XXI como combatê-la?.** Proelium – revista da academia militar, 2004.

BRANDÃO, P.; BRITO, V. **Terrorismo, inteligência e mecanismos legais: desafios para o Brasil.** In C.S. Arturi, ed. Políticas de defesa, inteligência e segurança. Porto Alegre: UFRGS Editora, 2014.

BRASIL. **Lei nº 10.744, de 9 de outubro de 2003.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/L10.744.htm>. Acesso em: 27 jul. 2017.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 27 jul. 2017.

BRASIL. **Lei nº 13.260, de 16 de março de 2016.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm>. Acesso em: 27 jul. 2017.

BONACCORSI, Daniela Villani. **O direito penal na sociedade de risco: uma análise da criminalidade econômica.** In: Homero Costa Advogados, Belo Horizonte - MG, Boletim Jurídico N.º 33 de 25 mar. 2011. Disponível em: <http://homerocosta.blogspot.com.br/2014/07/o-direito-penal-na-sociedade-de-risco.html>. Acesso em 02 ago. 2017;

CANETTI, Daphna; GROSS, Michael L.; VASHDI, Dana R.. **Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes.** Journal of Cybersecurity, Volume 3, Issue 1, 1 March 2017, p. 49 - 58, Disponível em: https://doi.org/10.1093/cybsec/tyw018. Acesso em: 09 ago. 2017.

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.

CASTRO, Henrique Hoffmann Monteiro de; COSTA, Adriano Sousa. **Lei antiterrorismo inova com a tentativa antecipada do crime.** Revista Consultor Jurídico**,** 20 de abril de 2016. Disponível em: <https://www.conjur.com.br/2016-abr-20/lei-antiterrorismo-inova-tentativa-antecipada-crime#author>. Acesso em: 22 nov. 2017.

CAVALCANTI, Sabrinna Correia Medeiros; GOMES, Olívia Maria Cardoso. **Lei antiterrorismo no Brasil e seus reflexos no estado democrático de direito.** XXVI Encontro Nacional Do CONPEDI Brasília – DF. P. 384 – 401.

CHAGAS, Morgana Santos das**. Ciberterrorismo: as possibilidades da expansão do terror nas relações internacionais.** 2012. 52f. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, João Pessoa, 2012.

CHOMSKY, Noam. **O império americano: hegemonia ou sobrevivência.** Trad. Regina Lira. Rio de Janeiro: Elsevier, 2004.

COLLIN, Barry C. **The future of cyber terrorism: where the physical and virtual worlds converge.** In: 11th Annual International Symposium on Criminal Justice Issues. Disponível em: <http://www.crimeresearch.org/library/Cyberter.htm>. Acesso em: 23 nov. 2017.

DENNING, Dorothy E. **Is Cyber Terror Next?** Disponível em: <http://essays.ssrc.org/sept11/essays/denning.htm>. Acesso em: 09 ago. 2017.

DIAS, Viriato Caetano. **De terrorismo convencional ao ciberterrorismo: um estudo de caso sobre o papel da Al-Qaeda.** Évora: Universidade de Évora, 2010.

DIONÍSIO, Bibiana; FONSECA, Alana; GIMENES, Erick. **Justiça condena oito réus da Operação Hashtag.** G1 PR, Curitiba. Pub. 04 mai. 2017. Disponível em: < https://www.conjur.com.br/2016-abr-20/lei-antiterrorismo-inova-tentativa-antecipada-crime#author>. Acesso em: 22 nov. 2017.

FIGUEIREDO, Wellington dos Santos; RAMOS, Elvis Christian Madureira. **Terrorismo: um legado histórico e sua caracterização na plataforma midiática.** Ciência Geográfica, Bauru, v. XVI, nº XVI, p. 195 – 216, pub. Jan/Dez, 2012.

FEKETE, Emily; WARF, Barney. **Relational geographies of cyberterrorism and cyberwar, Space and Polity.** 2016, p. 143-157. Disponível em: <http://www.tandfonline.com/doi/full/10.1080/13562576.2015.1112113>. Acesso em: 11 nov. 2017.

FOLHA DE SÃO PAULO. **Macron sanciona lei antiterrorismo, que substitui emergência na França.** Pub. 31 out. 2017. Disponível em: < http://www1.folha.uol.com.br/mundo/2017/10/1931704-macron-sanciona-lei-antiterrorismo-que-substitui-emergencia-na-franca.shtml>. Acesso em: 22 nov. 2017.

G1. **Ataque cibernético afeta serviços do Hospital do Câncer em Jales e Fernandópolis.** Pub. 27 jun. 2017. Disponível em: <https://g1.globo.com/sao-paulo/sao-jose-do-rio-preto-aracatuba/noticia/ataque-cibernetico-afeta-servicos-do-hospital-do-cancer-em-jales-e-fernandopolis.ghtml>. Acesso em: 22 nov. 2017.

G1. **Ciberataques em larga escala atingem empresas no mundo e afetam Brasil.** Pub. 15 mai. 2017. Disponível em: <https://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml>. Acesso em: 22 nov. 2017.

GARDINI, Mayara Gabrielli. **Terrorismo no ciberespaço: o poder cibernético como ferramenta de atuação de organizações terroristas.** Fronteira**,** Belo Horizonte, v. 13, n. 25 e 26, p. 7 – 33, 2014.

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: 23 nov. 2017.

JÚNIOR, Vladimir Vitti. **Análise da lei antiterrorismo (13.260/2016).** Revista Direito e Sociedade. v.4, nº 1. São Paulo: Universidade Zumbi dos Palmares, 2016.

Klein, John J.. **"Deterring and Dissuading Cyberterrorism."** Journal of Strategic Security 8, no. 4 - 23-38, 2015. Disponível em: http://scholarcommons.usf.edu/jss/vol8/iss4/2. Acesso em: 09 ago. 2017.

KUEHL, Daniel. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry (Ed.). **Cyberpower and national security**. Center for Technology and National Security Policy, National Defense University, Washington, 2009. Disponível em: <http://ctnsp.dodlive.mil/2009/04/01/cyberpower-and-national-security/>. Acesso em: 09 ago. 2017.

LACHOW, Irving. Cyber Terrorism: Menace or Myth. In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry (Ed.). **Cyberpower and national security.** Center for Technology and National Security Policy, National Defense University, Washington, 2009. Disponível em: < http://ctnsp.dodlive.mil/2009/04/01/cyberpower-and-national-security/>. Acesso em: 11 abr. 2015.

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, v.23, n. 53, p. 47-70, 2015.

MEDERO, Gema Sánchez. **Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. XXI.** Mérida: Universidad de Los Andes, 2012, p. 239-267. Disponível em: <https://canalcienciascriminais.com.br/o-papel-do-estado-no-combate-ao-ciberterrorismo/> . Acesso em: 09 ago. 2017.

MOREIRA, Adriano (coord). **Terrorismo.** 2ª ed. Coimbra: Almedina, 2004.

MCLUHAN, Marshall Et POWERS, Bruce R. **The Global Village - Transformations In World Life And Media In The 21st Century.** New York: Oxford University Press, 1989.

NELSON, Bill. **Cyberterror Prospects and Implications.** Naval Postgraduate School, Monterey, California, 1999.

NETO, Francisco Paulo de Melo. **Marketing do terror**. São Paulo: Editora Contexto, 2002.

PARKER, Amanda M. Sharp. Cyberterrorism: the emergent Worlwide Threat. In: CANTER, David. **The faces of terrorism: multidisciplinary perspectives.** Chichester: Ed. Wiley-Blackwell, 2009, p. 245-255.

PAYÃO, Felipe. **Segura essa: Brasil é o 4° país que mais sofre com o cibercrime.** Tecmundo. Pub. 27 abr. 2017. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/116181-segura-brasil-4-pais-sofre-o-

cibercrime.htm?utm_source=tecmundo.com.br&utm_medium=home&utm_campaign=tv>. Acesso em: 22 nov. 2017.

PINTO, Marco Aurélio Gonçalves. **Teoria relativista do ciberterrorismo.** Academia Militar: Departamento de estudos de pós graduados: Lisboa, 2011.

PRESSE, France. **França foi alvo de ao menos 10 atentados desde janeiro de 2015.** G1. Pub. 15 jul. 2016. Disponível em: <http://g1.globo.com/mundo/noticia/2016/07/franca-foi-alvo-de-multiplos-ataques-desde-janeiro-de-2015.html>. Acesso em: 22 nov. 2017.

SÁNCHEZ FRÍAS, Alejandro. **¿Cazador o presa en la telaraña del terror?: la ue en la lucha contra el ciberterrorismo.** Universidade de Málaga: Espanha, 2016. Disponível em: < https://riuma.uma.es/xmlui/bitstream/handle/10630/12586/Ponencia%20UC3M%20Alejandro%20Sanchez%20Frias.pdf?sequence=3> . Acesso em: 26 jul. 2017.

SANTOS, Eric de Assis. **Discutindo a terceira velocidade do direito penal**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 16, n. 2800, 2mar.2011. Disponível em: <https://jus.com.br/artigos/18603>. Acesso em: 10 ago. 2017.

SANTOS, Matheus; SOUZA NETO, Cícero Alves. **Crimes cibernéticos: generalidades e perspectiva da legislação brasileira.** Revista Transgressões: Ciências Penais em debate. V. 2, n. 1, p. 225 – 238, 2014. Disponível em: https://periodicos.ufrn.br/transgressoes/article/view/6664/5161**.** Acesso em: 09 ago. 2017.

TANGERINO, Dayane Fanti. **O papel do Estado no combate ao ciberterrorismo.** Canal Ciências Criminais. Disponível em: <https://canalcienciascriminais.com.br/o-papel-do-estado-no-combate-ao-ciberterrorismo/> . Acesso em: 26 jul. 2017.

TEIXEIRA, Ricardo Augusto Araújo. **Direito Penal de Emergência.** 2ª ed. Belo Horizonte: Editora D'Plácido, 2017.

VASCONCELLOS, Maria José Esteves de. **Pensamento sistêmico: o novo paradigma da ciência.** Campinas: Papirus, 2002.

VILELA, Pedro Correa Meyer. **Terrorismo: uma análise histórico-sociológica do fenômeno e crítica as táticas antiterror.** Artigos de Trabalhos de Conclusão 2014/1. PUCRS. Disponível em: <http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2014_1/pedro_vilela.pdf>. Acesso em: 01 out. 2017.

WEIMANN, Gabriel. **Cyberterrorism: How Real Is the Threat?** Special Research Report, Washington DC: United States Institute of Peace, 2004.

WIENER, Norbert. **Cibernética.** Tradução Prof. Gita K. Ghinnzeberg. São Paulo: Polígono e Universidade de São Paulo, 1970.