CIBERTERRORISMO: a internet como meio de propagação do terror

Danilo Henrique Nunes[1]
Lucas Souza Lehfeld[2]
Jonatas Santos Silva[3]

RESUMO: Devido a expansão e progressão tecnológica, bem como o uso intenso da *Internet*, foi possibilitado o surgimento de diversos crimes praticados no âmbito virtual, tais como o ciberterrorismo, seja na *Surface Web, Deep Web* ou *Dark Web* e, ainda, de como deverá ser aplicado o ordenamento jurídico brasileiro quando da incidência dos referidos crimes. Será feita apreciação da legitimidade para aplicação da Lei Antiterrorismo (Lei nº 13.260/2016), bem como um estudo de caso concreto da primeira aplicação efetiva da Lei. O método de pesquisa utilizado é o de revisão de literatura e hipotético-dedutivo, buscando referencial bibliográfico, através de artigos, críticas e reflexões, ponderando seu impacto no Direito Penal vigente. O tema, embora campo aberto e pouco discutido, aponta para a possível desestabilização do Estado em razão da propagação ao terror causado por essa cibercriminalidade, sendo necessária uma adequada abordagem devido ao grau de periculosidade, excepcionalidade e dimensão dos danos, com embasamento nos direitos fundamentais previstos na nossa Carta Magna.

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

ABSTRACT: Due to the technological expansion and progression, as well as the intense use of the Internet, it was possible the emergence of several crimes practiced in the virtual scope, such as cyberterrorism, whether on the Surface Web, Deep Web or Dark Web and, still, of how it should be the Brazilian legal system applied when the incidence of the aforementioned crimes. An assessment will be made of the legitimacy for applying the Anti-Terrorism Law (Law No. 13,260 / 2016), as well as a concrete case study of the first effective application of the Law. The research method used is the literature review and hypothetical-deductive, seeking a reference bibliographic, through articles, criticisms and reflections, considering its impact on the current Criminal Law. The theme, although open and little discussed, points to the possible destabilization of the State due to the spread of terror caused by this cybercrime, requiring an adequate approach due to the degree of dangerousness, exceptionality and extent of the damage, based on fundamental rights. provided for in our Charter.

Keywords: Cyberterrorism; Internet; Deep web; Dissemination of threat.

INTRODUÇÃO

Há cinquenta anos a *Internet* estava sendo projetada pelos militares nos Estados Unidos da América, com finalidades de manterem sua superioridade tecnológica durante a Guerra Fria. Entretanto, com o acesso expandido pela sociedade, tal avanço tecnológico

[1] Doutorando e Mestre em Direitos Coletivos e Cidadania pela Universidade de Ribeirão Preto/SP – Unaerp. E-mail: dhnunes@hotmail.com
[2] Pós-Doutor em Direito pela Universidade de Coimbra, Portugal. E-mail: lehfeldrp@gmail.com
[3] Especialista em Cências Criminais pela Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo, Usp. E-mail: jonatashet23@gmail.com

acarretou mudanças na nossa cultura. Esse invento chegou ao Brasil apenas 25 anos depois, revolucionando os meios de comunicação, bem como dinamizando as formas de atuação de setores públicos e privados, tornando a sociedade moderna submissa a esse âmbito digital. Claro que é indiscutível que a *internet* trouxe a proximidade da sociedade, reduzindo o tempo e o espaço. Nessa esteira, a *internet* também trouxe contrariedades quanto a censura e liberdade na relação entre cidadão e Estado, seja ele nacional ou internacional. Ademais, apesar dos benefícios proporcionados, o ciberespaço carrega questões contrárias quanto ao convívio em sociedade, no tocante ao estímulo de propagação de ideologias, bem como o terror fomentado na grande *World Wide Web,* precipuamente dentro da *Deep* e *Dark Web*. As vulnerabilidades que esse âmbito carrega, tornou possível a existência de diversos tipos de condutas danosas e, por esse motivo, termos como ciberguerra, ciberataque e ciberterrorismo tomaram espaço no ordenamento jurídico de vários Estados do globo.

Assim, o termo "ciberterrorismo" foi empregado pela primeira vez no ano de 1980 em um artigo redigido por Barry Collin (ALCÂNTARA, 2015), significando a junção do ciberespaço e do terrorismo convencional, para ataques conduzidos à longa distância, tornando a população refém do medo e ameaçando um Estado Democrático de Direito. Os respectivos danos causados por ciberterroristas no tocante à segurança do Estado advém da progressiva interdependência da sociedade moderna para com a tecnologia. Essa espécie de cibercriminalidade visa difundir o terrorismo comum no ciberespaço, abrangendo todo o âmbito transnacional para, eficazmente, disseminar o terror. Ademais, apresenta-se como objetivo principal de análise, uma adversidade em relação de como deve o ordenamento jurídico brasileiro ser aplicado diante um ataque desse porte. Tendo em vista as probabilidades de ocorrência do ciberterrorismo em esfera global, o presente estudo tem por escopo analisar as divergências entre essa modalidade de cibercriminalidade e terrorismo comum e de como deve o ordenamento pátrio abordar referido ato. Portanto, será feita uma análise acerca da legitimidade presente na Lei nº 13.260, de 16 de março de 2016 (Lei Antiterrorismo) para a adequada aplicação ao ciberterrorismo, assim como de demais normas esparsas presentes no ordenamento jurídico pátrio. Ademais, cumpre destacar que a referida Lei sofre críticas devido seu caráter de excepcionalidade perante o Código Penal vigente, confrontando princípios constitucionais. Desse modo, a presente pesquisa foi desenvolvida seguindo os métodos de revisão de literatura e hipotético-dedutivo, justificando-se que se partiu de uma concepção

abrangente de diversos autores para compreender o ciberterrorismo e sua forma de atuação, bem como seus impactos frente ao Estado e aplicação do Direito.

EVOLUÇÃO E PRINCÍPIOS NORTEADORES DA *INTERNET*

CONTEXTO HISTÓRICO: A INVENÇÃO DA *INTERNET* E A INCLUSÃO DIGITAL

Nem sempre a *Internet* existiu com todas as suas funções e tecnologias como conhecemos na atualidade. O marco inicial foi em setembro de 1969, com a elaboração e desenvolvimento da *Advanced Research Projects Agency Network* (ARPANET) criada pela *Advanced Research Projects Agency* (ARPA) do Departamento de Defesa dos Estados Unidos da América. Sendo assim, nesse momento é necessário fazer uma breve síntese sobre a história do projeto e desenvolvimento da ARPANET. Indubitavelmente, a *Internet* não foi fruto e inspiração de apenas uma única pessoa, Manuel Castells (2003, p. 28) afirma que "todos os desenvolvimentos tecnológicos decisivos que levaram à *Internet*, tiveram lugar em torno de instituições governamentais e importantes universidades e centros de pesquisa". No final da década de 50, com o lançamento pela União Soviética do satélite *Sputnik I* no auge da Guerra Fria, o Departamento de Defesa dos Estados Unidos sentiu-se ameaçado, criando logo em seguida a ARPA, uma agência militar de pesquisas com a finalidade de manter a superioridade tecnológica dos Estados Unidos e se prevenir contra avanços tecnológicos de potenciais adversários. Dessa forma, com o objetivo traçado, a ARPA anunciou o início da "Era da Informação" (POMPÉO; SEEFELDT, 2013) criando um sistema de comunicação a longa distância incapaz de se destruir com ataques nucleares ou sofrer extravios, permitindo a troca de dados e processamentos entre computadores.

Com efeito, a primeira rede de computadores denominada ARPANET teve suas funções iniciadas em setembro de 1969, portando seus quatro nós iniciais na Universidade da Califórnia em Los Angeles, no *Stanford Research Institute* (em português, Instituto de Pesquisa de Stanford), entre outras. Contudo, era preciso de uma invenção ainda maior para que a ARPANET realmente funcionasse de forma a capacitar que os computadores se conectassem uns aos outros. Assim sendo, a criação, em 1978, do conjunto de protocolos denominados *Transmission Control Protocol/Internet Protocol* (TCP/IP), bem como a

integração destes ao sistema *UNIX*, em 1983, resultaram na possibilidade de comunicação entre computadores, tornando-se protocolos padrões desde então. Com isso, tornou-se praticamente impossível desassociar a serventia da *Internet* para objetivos militares e científicos. Desta feita, foi em 1984 que ocorreu a divisão da rede em duas: Arpanet, uma rede com finalidade de pesquisas científicas civis, e a Milnet (*Military Network*), rede para instituições militares.

Na mesma década de 80 foram criados vários tipos de rede, contudo, todas tinham como base a ARPANET, uma vez que esta era a origem da rede. Nessa mesma época surgiu a rede principal, denominada *INTERNET*, operada pela *National Science Foundation* (NSF). Ademais, cumpre esclarecer o que é a "rede". Segundo Castells (2003, p. 7), "uma rede é um conjunto de nós interconectados", que criaram a denominada "teia virtual" assim formando a ARPANET e graças a ela temos a *Internet* como um enorme avanço nos dias atuais. Após vinte anos, a tecnologia da ARPANET ficou ultrapassada, tendo seu fim em 1990 por decisão dos militares, mantendo ativo apenas a MILNET. Dessa forma, as instituições que anteriormente pertenciam a ARPANET passaram a se interconectar à *National Science Foundation Network* (NSFNET), operada pela NSF, esta passando a ser o *backbone* (TECMUNDO, 2009) da rede de pesquisas civis. Em 1992, a NSF planejava a privatização da rede devido a proporção de sua expansão em escala global. Segundo estimativas de Coffman e Odlyzko (2013), o tráfego de dados na *Internet* era de cerca de 1TB por mês em 1990, 2 TB por mês em 1991, saltando para 16 em 1994, 1.500 em 1996 e 35 mil em 2000. Consequentemente, surgiram os primeiros provedores de acesso de forma a disponibilizar conexão ao público em geral. Ainda no ano de 1990, Timothy John Berners-Lee, cientista britânico, o qual era, na época, pesquisador no *Centre Européen poour Recherche Nucleaire* (CERN), desenvolveu a *World Wide Web* (*WWW*), dando amplitude à rede de forma que oferecesse aos usuários "um sistema fácil de pesquisa para procurar as informações desejadas"(CASTELLS, 2009, p. 88). No artigo científico publicado por Pompéo e Seefeldt, os autores explicam que a *WWW,* conforme abaixo descrito:

> [...] contém dados e informações que, armazenadas num servidor, podem ser exibidos por meio de hipertextos, vídeos, sons e imagens. Lidas através de um navegador, num espaço visível determinado, a internet, através de provedores de busca, direciona o usuário à páginas determinadas (POMPÉO; SEEFELDT, 2013).

Foi a partir de 1994 que a surgiu a *Internet* no território brasileiro para os usuários comuns (em 1988 já era liberado o acesso para as universidades brasileiras através na *Bitnet*, as quais se conectavam às redes internacionais). Contudo, o Ministério da Ciência e Tecnologia, almejando implementar uma rede que não precisasse de intermédio internacional, desenvolveu a Rede Nacional de Pesquisa (RNP), que conforme Bernardo Lins, teve estruturação custeada com recursos do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq e da Fundação de Amparo à Pesquisa do Estado de São Paulo – Fapesp (LINS, 2013). A administração pública contratou junto à Embratel uma estrutura básica de tráfego de dados, que iria configurar um *backbone* ou espinha dorsal da *Internet* brasileira. Nessa época, a Embratel estava por adquirir a monopolização do serviço de fornecer conexão à *Internet* ao público, porém, uma estratégia governamental de desestatização da economia impossibilitou com que a empresa continuasse seu empreendimento.

Surgiram, então, várias empresas que, mediante uma taxa, proviam o acesso à *Internet* por via telefônica com uso de um modem. Alguns anos mais tarde, o acesso remoto por linha discada progrediu para banda larga, findando com as falhas de conexão, garantindo maior velocidade, e consequentemente, o número de sites existentes na rede multiplicaram-se de forma que era impossível seu mapeamento. Deu-se, então, o surgimento do Google. A tecnologia da *Internet*, bem como os aparelhos celulares, computadores, *tablets,* desenvolveu-se com tamanha velocidade que foi capaz de adquirir uma vasta proporção, de modo que atualmente é quase utópico viver sem que tenhamos qualquer tipo de contato com ela, seja qual for as relações, ou seja, sociais e profissionais. É o que expõe a pesquisa feita pelo *We are social*, em 2019, que destaca que no Mundo há 4,19 bilhões de usuários na *Internet*, com um aumento de 9% em relação ao ano anterior. No tocante aos aparelhos eletrônicos, já são 5,11 bilhões de usuários móveis com acesso à *Internet* (WE ARE SOCIAL, 2019).

PRINCÍPIOS NORTEADORES DA *INTERNET*

Com o avanço da tecnologia e o desenvolvimento frenético da *Internet* na metade do século passado, bem como a acessibilidade desses meios à população mundial, fez-se necessário a elaboração de princípios e direitos para a sua governança. Assim, após 1980, entidades não governamentais subordinadas ao Governo dos Estados Unidos, tais como a

ICANN (*Internet Corporation for Assgined Names and Numbers*) e a IANA (*Internet Assigned Numbers Authority*), se incumbiram de regulamentar a *Internet* (KRETSCHAMANN; WENDT, 2018, p. 153-154). Em 2001, a ONU (Organização das Nações Unidas) editou a Resolução 56/183 para estabelecer um novo modelo de Governança na *Internet*. Em 2003 ocorreu a primeira conferência, realizada em Genebra e, em 2005, teve a segunda realizada na Tunísia (KRETSCHAMANN; WENDT, 2018, p. 153-154). Dessa forma, através da regulação, a governança da *Internet* empenha-se a proteger a individualidade dos Estados-Nação, os direitos humanos e sociais, tais como a privacidade e proteção de dados, liberdade de expressão, entre outros.

CARTA DE DIREITOS HUMANOS E PRINCÍPIOS PARA A *INTERNET*

Na *Internet* existe uma plataforma global denominada *Internet Governance Forum* – Fórum de Governança da *Internet* (IGF), em português. Essa plataforma, instituída em 2006, é um fórum aberto onde reúne diversas pessoas com interesses em comum por meio de discussões a respeito de políticas públicas relacionadas a *Internet*, aspectos técnicos, comerciais, sociais e administrativos (INTERNET GOVERNANCE FORUM), visando melhorias e o crescimento da *Internet*. O IGF é sempre convocado pelo Secretário-Geral da ONU, com o apoio do Secretariado do IGF, para executar o mandato emitido na Cúpula Mundial sobre a Sociedade da Informação. Nesse processo, é quando ocorrem as reuniões para debate das questões de política pública relacionadas à governança da *internet*. Na primeira reunião da Cúpula Mundial, foram formados dois acordos para que fossem empregados os direitos humanos para a governança da *Internet*. O primeiro, denominado *Bill of Rights Dynamic Coalition*, tinha como objetivo elaborar uma Carta de Direitos Humanos e o segundo, *Framework of Principles for the Internet Dynamic Colation*, com a finalidade de versar a respeitos de princípios de governança da rede. Sendo assim, no início do ano de 2009, esses dois acordos foram agrupados para formar a Coalizão Dinâmica de Direitos e Princípios da *Internet*, consubstanciando os direitos humanos e princípios para que sejam aplicados no âmbito da rede. Como resultado foi elaborada a Carta de Direitos Humanos e Princípios da *Internet*. A Carta de Direitos Humanos e Princípios para a *Internet* possui embasamento na Declaração Universal dos Direitos Humanos e outros tratados que constituem a Carta Internacional dos Direitos Humanos da Organização das Nações Unidas. Ou seja, é um documento por meio do qual

conscientiza os usuários de que também possuem direitos no âmbito online, integrando dez princípios.

O princípio, denominado “universalidade e igualdade” traz o mesmo conceito do previsto na CRFB/1988, artigo 5º, significando, portanto, que “todos os indivíduos são iguais em dignidade e direitos que devem ser respeitados” e cumpridos no meio *online*. O Princípio “Direitos e justiça social” prevê que no âmbito da *Internet* todos os usuários devem respeitar os direitos humanos, sendo um espaço para promover, proteger e cumprir referidos direitos. Nesse sentido, o Princípio da Acessibilidade garante o direito de acesso e utilização de rede aberta e segura a todos os indivíduos. No que tange o Princípio da Expressão e Associação, é garantido a todas as pessoas o acesso para pesquisas e recebimento de informações via rede mundial, bem como para divulgação de tais informações. Além disso, é assegurado o direito de associação no âmbito online, para fins sociais, políticos, culturais ou outros (INTERNET RIGHTS AND PRINCIPLES COALITION, 2019). Ademais, os usuários possuem o direito à privacidade e ao anonimato, podendo utilizar-se da ferramenta de criptografia, bem como possui o direito à proteção de dados, tendo o controle sob a divulgação, retenção ou eliminação de dados pessoais, conforme dispõe o Princípio da Privacidade e Proteção de dados. A denominação do sexto princípio – vida, liberdade e segurança – é autoexplicativa, uma vez que o direito à vida, à liberdade e à segurança também devem ser respeitados e protegidos no âmbito online, contudo esse princípio traz o dever de que os usuários não utilizem tais direitos para violar outros previstos para a *Internet*.

A inovação técnica e política na rede deve ser estimulada, de forma a promover a diversidade cultural e linguística, facilitando a pluralidade de expressão no âmbito online, conforme estabelece o Princípio da Diversidade. O nono e penúltimo Princípio da Carta, nominado “Padrões e Regulamento”, determina que deve sempre utilizar como base os padrões abertos para sistema de comunicação, documentos e dados, visando a interoperabilidade, inclusão e igualdade para todos os usuários da rede. Por fim, o Princípio da Governança dispõe que os direitos humanos e a justiça social serão garantidos por meio de um governo, na *Internet*, multilateral e transparente, tendo como embasamento os princípios de abertura, participação inclusiva e de responsabilização.

COMITÊ GESTOR DA *INTERNET* NO BRASIL E OS PRINCÍPIOS PARA A GOVERNANÇA E USO DA *INTERNET*

A rede expandiu somente após a criação da *World Wide Web*, em 1990, por Tim Berners-Lee, quando se tornou popular e utilizada mundialmente, não só para fins militares e pesquisas científicas. Contudo, somente em 1995 que a *Internet* passou a ser usual no Brasil, sendo criado o Comitê Gestor da *Internet* no Brasil, através da Portaria Interministerial (MCT/MC) nº 147/1995, alterada pelo Decreto Presidencial nº 4.829/2003. Este Comitê possui a atribuição para estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da *Internet* no Brasil, coordenando os endereços da rede (IPs) e do registro de nomes de domínios utilizando ".br" (PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNE**T)**, promove estudos e procedimentos para a segurança da *Internet* e seus usuários. No ano de 2005 todas as atribuições técnicas e operacionais do CGI foram delegadas para o Núcleo de Informação e Coordenação do Ponto BR (NIC.br). Essa entidade possui natureza jurídica de direito privado e sem fins lucrativos, tendo a atribuição de prover a infraestrutura e recursos necessários à atuação do CGI. Em 2009, de forma a resguardar os princípios fundamentais previstos na Carta Magna, o Comitê Gestor da *Internet* no Brasil aprovou a Resolução nº 003, estabelecendo dez Princípios para a Governança e Uso da *Internet* no Brasil, quais sejam : a) liberdade, privacidade e direitos humanos; b) governança democrática e colaborativa; c) universalidade; d) diversidade; e) inovação; f) neutralidade da rede; g) inimputabilidade da rede; h) funcionalidade, segurança e estabilidade; i) padronização e interoperabilidade; j) ambiente legal e regulatório.

DO TERRORISMO AO CIBERTERRORISMO

DEFINIÇÕES ACERCA DO TERRORISMO CONVENCIONAL

Os atentados ao *World Trade Center*, em 11 de setembro de 2001, nos Estados Unidos da América, dataram o maior ataque já sofrido por esse país que detinha a posição de ser o mais forte no contexto internacional. Consta que nesta data, dezenove agentes do grupo *Al Qaeda*, comandado por Osama bin Laden, sequestraram quatro aeronaves

americanas para iniciar o atentado, ocasionando quase três mil mortes. As três aeronaves lograram êxito ao atingir as Torres Gêmeas e o Pentágono, porém a quarta aeronave caiu em uma área rural na Pensilvânia antes de atingir o seu alvo, graças a revolta dos passageiros (OPOVO ONLINE, 2018).

A relevância do fato, reproduzido através da mídia – na época por meio de televisões, causou grande impacto internacional e disseminou o medo. Conforme relata Almeida *et al* (2017, p. 73), "a questão, então, passou a ocupar não só a agenda dos operadores do Direito, mas também da população em geral e dos *mass media"*. Entretanto, atualmente o terrorismo não possui um conceito jurídico homogêneo no âmbito global, abrangendo divergências e ambivalências, uma vez que cada país atribui um sentido técnico-legal ao fato. Assim, foram realizadas diversas assembleias pela ONU com objetivo de determinar um conceito para o terrorismo. Contudo, como era de se esperar, referido objetivo não obteve resultado, tendo em vista as diferenças históricas, geográficas, políticas e ideológicas que caracterizam cada um dos Estados integrados. Diante isso, cada país busca tratar e conceituar o tema de acordo com a realidade vivenciada, elucidando as diversas concepções de classificar o terrorismo, sendo, desse modo, criado uma pluralidade de designações acerca do tema. Porém, consoante a Resolução nº 1566, de 8 de outubro de 2004, adotada Conselho de Segurança das Nações Unidas, o terrorismo pode ser compreendido como:

> [...] atos criminosos, nomeadamente aqueles dirigidos contra civis com a intenção de causar a morte ou lesões corporais graves ou a tomada de reféns com o objetivo de provocar um estado de terror na população em geral, em um grupo de pessoas ou em determinadas pessoas, de intimidar uma população ou de forçar um governo ou uma organização internacional a realizar ou abster-se de realizar qualquer ato [...] (UNITED NATIONS SECURITY COUNCIL, 2004)

Apesar de não haver um consenso quanto ao conceito, estudiosos do assunto afirmam que "o elemento central desta 'macrocriminalidade' ou 'criminalidade expressiva', é a participação do agente em uma organização com fins terroristas." (ALMEIDA et. al., 2017, p.27). Dessa forma, o terrorismo seria uma espécie de crime organizado, mesmo que alguns agentes atuem de modo individual. Desse modo, a definição de organização terrorista é fundamental para tipificação do fato. Zygmunt Bauman descreve que de forma ideal tal assertiva:

> Os rebeldes não constituem uma organização cujos membros "cumpram diligentemente ordens vindas de cima", mas uma "ampla série de grupos menores que frequentemente atacam por iniciativa própria ou se juntam para um único atentado. A "estrutura" (se é que se permite usar esse termo) "é **horizontal, e não hierárquica, e *ad hoc* em vez de unificada**" (BAUMAN, apud ALMEIDA et. al., 2017, p. 28).

Portanto, essas organizações não são homogêneas, sendo difícil identificar um terrorista, apesar de já existir um senso comum e uma imagem social. Nesse sentido, descreve-se que:

> o terrorismo vem da pobreza, de famílias desfeitas, da ignorância, da imaturidade, da falta de responsabilidades familiares ou profissionais, de mentes fracas suscetíveis à lavagem cerebral – sociopatas, criminosos, fanáticos religiosos [...] ou, ainda, de indivíduos [...] simplesmente maus (SAGEMAN apud ALMEIDA et al, 2017, p. 29).

Dessa forma, há autores que defendem que o terrorismo compreende atos de protesto contra a injustiça social, como no caso do atentado ao *World Trade Center*, tendo sido os responsáveis considerados agentes da justiça. Nesse sentido, a pobreza e opressão seriam os fatos geradores do terrorismo (PINTO, 2011). Contudo, Sageman (apud ALMEIDA et al, 2017, p. 29) venceu tais estereótipos ao estudar biografias de quatrocentos terroristas pertencentes ao grupo Al Qaeda e constatar que:

> ¾ da amostra integrava a classe alta ou média; 63% tinham acesso a universidade; ¾ tinham profissão, muitos deles engenheiros ou arquitetos (neste ponto relembrou que Bin Laden era engenheiro civil, Zawahiri era médico e Mohamed Atta, arquiteto); boa parte sabia dois ou três idiomas ocidentais (alemão, francês, inglês); 90% vieram de famílias bem estruturadas e afetuosas; 73% eram casados e, em sua grande maioria, já tinham filhos (os que não eram casados eram muito jovens para tanto); muitos só se tornaram religiosos após ingressas na *jihad* (isto é, na luta); apenas 13% frequentaram a madraça (escola de estudos corânicos); a maioria não possuía antecedentes criminais; não eram solitários; e somente 1% apresentava indícios de distúrbios mentais.

Isto posto, a imagem social criada de que terroristas são muçulmanos, analfabetos, homens-bomba e que vivem em um lugar isolado, planejando ataques violentos e sanguinários não passa de um mero pré-conceito midiático. Nesse sentido, afirma-se que:

> O terrorismo é mostrado como uma característica quase inerente ao Islã, e até mesmo elemento mais importante dele – retratando-o como uma religião hostil e militarista cujo principal objetivo é o "espalhar pela espada". Atenção também é dada a táticas terroristas como o bombardeio suicida e o assassinato de pessoas inocentes e foco também é colocado sobre a ameaça específica para a América e outros países do Ocidente daqueles que seguem "jihad"(AGUILERA-CARNERERO; AZEEZ apud MARQUES; GONTIJO, 2019).

Importante ressaltar que, puramente, a "*jihad*" é um conceito religioso significando "o maior esforço possível pela Causa de Deus", seguido por muçulmanos. Entretanto, é confundido no termo com a *qital*, a qual faz referência a guerra e combate armados, sendo a *jihad* interpretada e empregada de forma errônea pelos grupos terroristas (CARTA CAPITAL , 2017). Nessa perspectiva, Dan Verton (apud ALCÂNTARA, 2017) já preconizava nos anos 2000:

> A próxima geração de terroristas não será uma horda de bandidos acéfalos vivendo no aperto existente no Afeganistão. As jovens crianças que eles estão radicalizando hoje estão estudando matemática, ciência da computação e engenharia. Eles crescerão e perceberão "Eu sou muito valioso para colocar dinamite ao redor da minha cintura e caminhar até um café lotado" [...]. "A Internet será outra ferramenta na sua caixa de ferramentas".

Em suma, atualmente não há um perfil uno de terroristas para que se possa identificá-los, uma vez que não mais correspondem aos referidos estereótipos. Ainda, devido ao avanço da tecnologia, a prática do terrorismo é passível de inutilização de armas de fogo, como por exemplo, a interferência ou manipulação de serviços de controle de aeronaves, causando um desastre de grande proporção e dizimando inúmeras vidas. Com esse exemplo, traz consigo o crime de ciberterrorismo, pois, conforme se verá nessa pesquisa, trata-se de ações desprovidas de armamentos, contudo, de extrema violência e relevância.

O CIBERESPAÇO E AS DOBRAS SEMIÓTICAS

No contexto de ciberespaço, existem inúmeras definições trazidas por estudiosos do tema. Lévy (1999, p. 92), filósofo e sociólogo francês, define como "o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos

computadores". Outra definição é feita por Kuehl (apud GARDINI, 2014), o qual entende que o ciberespaço se traduz em:

> 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 [...].

Sumariamente, todo o espaço digital navegável, bem como passível de trocas de informações e comunicações, através da rede, constitui o denominado ciberespaço. Contudo, o ciberespaço não é exclusivamente atingido através de um computador, como determina Lévy, uma vez que na atualidade, encontra-se presente em distintas máquinas como, por exemplo, *tablets,* aparelhos celulares e as recentes *Smart TVs*. Destaca-se:

> O ciberespaço cria linhas de fuga e desterritorializações, mas também reterritorializações [...], nos coloca em meio a diversos problemas de fronteira, agravando as crises de controle de acesso, influindo em todas as demais formas de desterritorializações contemporâneas. A desterritorialização informacional afeta a política, a economia, o sujeito, os vínculos identitários, o corpo, a arte. A internet é, efetivamente, máquina desterritorializante sob os aspectos políticos [...], econômico [...], cultural [...] e subjetivo [...]. Estão em marcha processos de desencaixe e de compressão espaço-tempo (LEMOS, André apud CARVALHO, 2019).

Ainda, entende-se que os atos praticados no ciberespaço não são exclusivamente cibernéticos, ou seja, também podem efetivar-se no espaço físico, tendo sido ele utilizado como uma ferramenta ou não. Destarte, Nye Júnior (apud GARDINI, 2014) interpreta o ato cibernético como "a capacidade para obter resultados preferidos mediante o uso dos recursos de informação eletronicamente conectados do domínio cibernético". Por conseguinte, é no ciberespaço em que encontramos as *Webs* e suas dobras. A *WWW* é composta por elos (*links*), páginas e navegadores que funcionam por meio da conexão com a *Internet*, como já explicado no tópico anterior. Com efeito, a *WWW* se desdobra, resumidamente, em três níveis: *Surface Web*, *Deep Web* e *Dark Web*. Foi em 1994 que se considerou pela primeira vez a divisão da web em visível e invisível, tendo sido esse entendimento advindo de Esworth (CALDERON, 2017, p. 217). A dobra visível do ciberespaço, denominada *Surface Web* ou *Web* Visível, é aquela em que todos tem acesso facilmente e pela se faz uso diário por meio de *sites* como o *Google*, *Yahoo!,* etc. Todo o conteúdo presente na *Surface* é indexado e é por esse motivo que são visíveis aos usuários

comuns. Assim, a *Web* visível é composta por páginas que foram reconhecidas pelos motores de busca convencionais, como o *retro* mencionado *Google*, e *a posteriori*, armazenadas em um banco de dados próprio do servidor. Portanto, quando o usuário realizar uma pesquisa na plataforma desse motor de busca, o conteúdo que fora indexado será resgatado e demonstrado em uma listagem.

O termo "*Deep Web*" (em português, *web* profunda) foi criado por Bergman, em seu trabalho publicado em 2001 pela empresa *Bright Planet*. Em sua pesquisa, Bergman (2001) faz um estudo acerca da dimensão dessa parte da *WWW* e, ainda, supõe que a *web* profunda possui aproximadamente 10 níveis, de modo que o acesso seja diferente em cada um deles, devendo ser feito de forma gradual. Destaca-se assim que a *Deep Web* e a *Dark Web*, são níveis da *World Wide Web* que representam a dobra invisível no ciberespaço, constituindo-se por todas as páginas que não foram – ou não puderam ser – indexadas pelos motores de busca. Existem inúmeros motivos para que as páginas não sejam indexadas, podendo ser por opção de privacidade de seu dono; por dificuldade de distinguir se uma página possui programa automático (*scripts*) para geri-la de forma benéfica ou maligna; ou até mesmo por violar regras dos próprios motores, uma vez que não é admitido a indexação daquelas que abranjam conteúdo impróprios, acessos a informações confidenciais, entre outros.

Ainda, dentro da pesquisa realizada por Bergman, o autor constatou que a *Deep Web* era entre 450 a 550 vezes maior do que a *Surface Web*, sendo, portanto, a dobra da *Web* que mais cresce. Ademais, aproximadamente 94,7% das páginas dessa dobra da *Web* são abertas, ou seja, sem restrições de qualquer tipo para acesso (CALDERON, 2017, p. 220). Em muitos estudos os termos *Deep Web* e *Dark Web* são utilizados como sinônimos, porém, ambas compreendem camadas da *Web*. A *Deep Web* possui quatro dobras e, entre ela, situa-se a *Dark Web*. A maneira mais fácil de explicar as camadas da *Word Wide Web* é por meio da analogia a um *iceberg*: a ponta superficial, aquela que é visível, refere-se a *Surface Web*, enquanto a parte mais profunda, invisível pelo mar, seria a *Deep Web* e a *Dark Web*.

Diversos ensaios relatam que esse lado obscuro da *Web* é demasiadamente utilizado pela garantia de privacidade, uma vez que na *Surface* o bombardeio de propagandas origina-se a partir de uma simples busca. Em contraste, uma porção abundante de criminosos praticam atos ilícitos mais facilmente na *Dark Web* devido a garantia de anonimato da rede. Referida rede teve origem em uma tese de doutorado, intitulada

"*Distributed Decentralised Information Storage and Retrieval"*, de Ian Clarke, em 1999 na Universidade de Edimburgo, localizada na Escócia. Ao colocar em prática sua tese, em 2000 deu-se início ao projeto de um *software* denominado *Freenet*. O objetivo do projeto de Clarke era permitir que seus usuários compartilhassem informações e dados entre si de forma totalmente anônima. Foi, portanto, desenvolvido e passou a funcionar em uma plataforma *peer-to-peer*, ou seja, cada usuário, para ter acesso, deve disponibilizar largura de banda e uma parte do disco rígido do seu aparelho. Assim, essa parcela disponibilizada ficaria acessível aos demais usuários da rede para armazenar informações criptografadas.

Segundo consta no site do *Freenet Project*, a rede é um "*software* gratuito que permite compartilhar arquivos anonimamente, navegar e publicar '*freesites*' (sites acessíveis apenas pela *Freenet*) e conversar em fóruns, sem medo de censura" (FREENET PROJECT, 2019). Atualmente tanto o *software The Onion Router* (TOR) quanto a *Freenet* representam redes da *Darknet* que, por meios de URL corretas, possibilitam o acesso tanto à *Deep* quanto à *Dark Web*. Entretanto, a rede TOR é a mais utilizada, devido a proteção em camadas criptografadas. Portanto, conforme explicitado até o momento, a *Dark Web* representa uma parte dentro da *Deep Web*, na qual as páginas não podem ser indexadas pelos motores de busca e pretendem permanecer alheias a eles, de forma a garantir o completo anonimato e a privacidade dos usuários por meio das redes TOR e *Freenet* para lograr referido objetivo. Devido a comercialização da *Internet* e o aumento de usuários, bem como a grande quantidade de troca de informações, cresceu também o índice da cibercriminalidade graças ao estimulo de manter o sigilo pelo anonimato garantido nas redes profundas. Nessa esteira, agentes do ciberterrorismo viram nesse âmbito um meio propício para ataques. Mesmo que as narrativas influenciadoras do ciberterrorismo também se encontrem na *Surface Web*, importante destacar a utilidade desses dois níveis da WWW, uma vez que oferece uma facilitação para suas atividades, tal como o almejado anonimato pela criptografia, no que tange a troca de informações dos participantes do grupo. Nesse sentido:

> Essa movimentação em plataformas digitais é muito bem orquestrada e se utiliza principalmente das ferramentas de anonimato que o ciberespaço permite, principalmente o espaço da *DeepWeb* e *Dark Web* e a facilidade de acesso a mecanismos como VPN/GhostVPN, Tor (*The Onion Router*) e serviços de e-mail criptografados, como o *Bitmessage* (ATWAN apud ALCÂNTARA, 2017).

Entretanto, ainda que não ocorrido um terrorismo cibernético deveras grandioso através da *Dark Web*, aponta Nye Júnior que o "domínio virtual permite aos terroristas: [...] operar como redes de franquias descentralizadas, criar uma imagem da marca, recrutar partidários, levantar fundos, proporcionar manuais de treinamento e controlar operações" (NYE JÚNIOR apud GARDINI, 2014). Não se pode anular as possibilidades de que ciberterrorismos ocorram utilizando-se da rede, e, muito menos, negar que não seja utilizada para aperfeiçoamento na atuação de grupos terroristas, bem como organização e elaboração de um ciberataque. Desse modo, os direitos à vida e à segurança são garantidos nos artigos 5º e 144, ambos da Constituição Federal, sendo responsabilidade do Estado garantir o bem-estar e proteção da população.

CONCEPÇÕES E MEIOS DE ATUAÇÃO DO CIBERTERRORISMO

No cenário do século atual, diante a inclusão digital, é possível demonstrar diversos setores que estão vinculados à rede e que dependem desse sistema para funcionar. Só para ilustrar, a prestação de serviços essenciais e vitais à vida humana, tais como energia, transporte, saúde, telecomunicações, estes estão sujeitos ao âmbito virtual (ALMEIDA; CUNHA, 2017). Diante essa perspectiva, torna-se fácil compreender o terror e o medo que predomina quanto a uma ameaça ciberterrorista. Nesse ínterim, após explanar brevemente a respeito do terrorismo e ciberespaço, necessário saber o que é ciberterrorismo. Apesar das tentativas de defini-lo ainda paira divergências entre os estudiosos do tema, assim como ocorre com o terrorismo comum, não havendo consenso quanto ao seu conceito. Em 1980, em um artigo redigido por Barry Collin, o termo "ciberterrorismo" foi empregado pela primeira vez para se referir à junção do ciberespaço e do terrorismo. Portanto, segundo o autor, o ciberterrorismo significa o

> Perigo de ataques conduzidos à longa distância (como consequência da interseção entre mundo físico e virtual) e tendo como alvos infraestruturas críticas de um país (fazendo com que a população de um país não conseguisse "comer, beber, se locomover, ou viver") (ALCÂNTARA,2017).

O termo foi utilizado novamente no final de 1990, em uma reunião do Grupo dos 8 realizada na França, na qual foi avaliado e discutido os crimes instigados por intermédio de

aparelhos eletrônicos e disseminação de informações via *internet*. Um pouco mais tarde, no ano de 2001, foi definido uma pesquisa o termo ciberterrorismo como sendo:

> Ataques ilegais e a ameaças de ataques contra computadores, redes e informações nele armazenadas quando feitos para intimidar ou coagir um governo ou seu povo em prol de objetivos políticos ou sociais. Além disso, para se qualificar como ciberterrorismo, um ataque deve resultar em violência contra pessoas ou propriedade, ou pelo menos causar danos suficientes para gerar medo. Ataques que levam à morte ou lesões corporais, explosões ou perda econômica grave seriam exemplos. Ataques graves contra infraestruturas críticas podem ser atos de ciberterrorismo, dependendo do seu impacto. (DENNING apud ALMEIDA; CUNHA, 2017).

Portanto, entende-se que o ciberterrorismo refere-se ao uso de aparelhos eletrônicos conectados à *Internet* para a prática de atos ilegais, com o intuito de causar terror e graves prejuízos a um Estado ou em um grande número de pessoas. Neste sentido:

> Um ato de ciberterrorismo ocorre quando um indivíduo ou organização usa uma rede de computadores para sobrecarregar e destruir um sistema nacional de gerenciamento de energia. Todavia, não ocorre quando um suicida destrói uma rede elétrica; nem ocorre se um terrorista usar a World Wide Web para adquirir informações sobre a construção de uma arma química. (CHE apud ALMEIDA; CUNHA, 2017).

Sob esse prisma, Awan (apud ALCÂNTARA, 2015) esclarece que "dado tipos de comportamento podem ser ligados a problemas e movimentos sociais, isso nos permite olhar para o ciberterrorismo através das lentes da mudança social". Nesse sentido, Carrapiço explica que cibercrime "[...] é a denominação dada a um conjunto específico de crimes relacionados com a utilização de computadores e de redes informáticas" (CARRAPIÇO apud ALMEIDA; CUNHA, 2017). *Stricto sensu,* o cibercrime refere-se ao cometimento de delitos em desfavor dos sistemas de informática, enquanto *lato sensu*, os recursos de meios informáticos apenas facilitam o delito. Portanto, os crimes cibernéticos e ciberterrorismo estão contidos na modalidade *lato sensu*, diferenciando-se apenas pelo elemento subjetivo que comportam. Ainda, necessário se faz distinguir o ciberterrorismo da ciberguerra, vide:

> 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 [...] (MEDERO apud COSTA, 2017).

Portanto, o ciberterrorismo traduz-se em um ataque cibernético com o fim de causar pânico, medo em uma sociedade e provocar graves prejuízos a um Estado, por diversos motivos, enquanto a ciberguerra consiste em uma agressão cibernética de Estado para Estado. Um exemplo de ciberguerra é o conhecido "caso da Estônia", quando o país sofreu um ataque cibernético generalizado, acarretando num colapso no sistema informático do Parlamento, Ministérios, bancos e jornais em 2007, tendo sido a Rússia acusada de determinado feito (O GLOBO). Os agentes do ciberterrorismo são denominados ciberterroristas e não se confundem com os *hackitivistas*, pois estes não atentam contra serviços essenciais à humanidade, não possuem objetivo de ataques com o intuito de aterrorizar e ferir pessoas, mas apenas visam protestar. Como exemplo de *hacktivismo*, podemos citar a plataforma *Wikileaks*. Essa página se compara à enciclopédia online *Wikipédia*, localizada na Surface, cujo termo "*leaks*" traduzido ao idioma português significa "vazamento" (CALDERON, 2017).

Embora exista um endereço para o *Wikileaks* na superfície da *Web*, sendo alguns documentos visíveis a qualquer usuário que acessar, também existe uma página não indexada dessa organização, de forma que arquivos confidencias são encontrados por lá. Da mesma forma, a comunicação de denunciantes com a organização só ocorre por meio da *Dark Web*, pelo fato da existente garantia do anonimato, prevenindo-se o controle por parte do governo. O objetivo principal dessa organização é fazer com que determinados temas sejam levados ao conhecimento público, mesmo que certas informações feitas por denunciantes sejam de extremo sigilo. Assim sendo, os *hackitivistas* através da *Wikileaks* disponibiliza conteúdos que envolvem matérias a respeito de guerra, governo, corrupção e espionagem (CALDERON, 2017). Ao contrário dos *hackitivistas*, os ciberterroristas possuem como objetivo primordial atentar contra a infraestrutura de Estados e seus serviços essenciais à sobrevivência humana, acarretando lesão, morte e, sobretudo, pânico na sociedade. Posto isto, imprescindível se faz visualizar as inúmeras vantagens para os cibertorristas, uma vez que a diversidade e a multiplicidades de alvos que podem atingir são enormes. Dentre elas, existe a possibilidade que esses coatores encontrem fraquezas

nos sistemas para poderem explorar e, consequentemente, causar danos. Weimann (apud CHAGAS, 2013) apresenta outra vantagem:

> Ciberterrorismo pode ser realizado remotamente, uma característica que é especialmente atraente para terroristas, pois o ciberterrorismo requer menos treinamento físico e investimento psicológico, porque o risco de mortalidade das formas convencionais de terrorismo é aqui excluído [...].

Desta feita, por intermédio de aparelhos eletrônicos conectados à *Internet*, a finalidade dos ciberterroristas, segundo Batista, Ribeiro e Amaral (apud COSTA, 2017) é "desestabilizar política, ideológica ou financeiramente um grupo, organização ou governo, utilizando a *internet* para perpetrarem as ações consideradas necessárias". Por certo, a propagação do terror tornou-se fácil devido ao ciberterrorismo, uma vez que os ataques podem ser realizados em um curto lapso temporal. Ainda, ciberterroristas podem causar grandes impactos e danos à sociedade moderna, a qual está cada dia mais submissa à tecnologia. Uma das estratégias empregadas pelos ciberterroristas é o *Denial Of Service Attack – DoS attack* (CALDERON, 2017), por meio do qual os servidores da web são invalidados devido à sobrecarga. Assim, vários danos podem ser causados enquanto servidores de energia elétrica ou setores produtivos industriais, encontrarem-se indisponíveis para os seus utilizadores.

Collin (apud CHAGAS, 2013) ilustra alguns casos prováveis de ciberterrorismo. Segundo ele, um usuário é capaz de invadir o sistema de controle de uma fábrica de cereais e adulterar os níveis de complemento do mineral de ferro, podendo acarretar intoxicação e morte dos indivíduos que consumirem referido produto. Outra hipótese seria o incurso nos sistemas de controle tráfego aéreo com o intuito de causar colisões entre aeronaves não particulares, com o dolo de atingir um número maior de pessoas. Ademais, um experimento realizado em 2007 no *Idaho National Laboratory* (em português, Laboratório Nacional de Idaho) constatou a real possibilidade de se utilizar da tecnologia para realizar esse tipo de ataque, conforme descreve Barney Warf e Emily Fekete (apud COSTA, 2017):

> 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 infraestrutura 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.

Contudo, ainda que o ciberterrorismo não seja passível de realização por usuários comuns, devido a incapacidades destes, a ameaça ciberterrorista não deve ser ignorada. Além disso, carece de um planejamento, restando evidente o dolo na conduta do agente, com o fim de causar o terror e desestabilizar o Estado.

MUNIÇÕES DOS CIBERTERRORISTAS

Uma das formas mais comuns da prática ciberterrorrista é por meio do uso de vírus informáticos, os quais, após criado, se propagam automaticamente atingindo outras aplicações no computador e causando danos no aparelho. Atualmente, existem diversos antivírus no mercado digital para combater tais males, contudo, com o avanço tecnológico, criminosos desta seara estão cada vez mais melhorando e evoluindo o software malicioso para que seja difícil ou, quase nula, sua detecção. O primeiro *virus hoax* surgiu em meados de 1988, com a função de se propagar via e-mail e atingir diversos destinatários, pois, quando uma vítima era atingida, recebia uma notificação arraigada de ameaças acerca de um falso vírus (PINTO, 2011). Já os *trojans* (cavalos de Tróia) são clássicos no âmbito da *internet*, configurando outra forma de ataque informático. Sua característica consiste na transferência e execução pelos próprios usuários do *software*, pois confundem-se com ficheiros comuns e inofensivos – como, por exemplo, jogos baixados no computador. Assim, uma vez executados, "alteram as configurações do sistema operativo e abrem *backdoors* para que os criminosos entrem nos computadores infectados de forma a obter controlo sobre eles, podendo roubar/destruir/adulterar informação confidencial' (PINTO, 2011). Como terceiro e último exemplo de formas vinculadas à prática ciberterrorista, temos o *phishing*, um meio para tentar adquirir informações pessoais do usuário informático para depois serem usados contra a própria vítima. As mensagens de *phishing* aparentam ser inofensivas, uma vez que

> parecem ser enviados por organizações legítimas como PayPal, UPS, uma agência do governo ou seu banco; entretanto, elas são em fato falsas mensagens. Os e-mails pedem de forma educada por atualizações, validação ou confirmação de informações da sua conta, sempre dizendo que houve algum problema. Você é então redirecionado a um site falso e enganado a

> apresentar informações sobre a sua conta, que podem resultar em roubos de identidade (AVAST).

Diante dessa forma de atuação com o intuito de levar o usuário a erro, mediante a alteração do *design* dos *sites* e com a inserção dos dados pessoais pela própria vítima, tais dados são furtados pelos criminosos e, posteriormente, utilizados para si e, financiamento de do ciberterrorismo(PINTO, 2011). Tendo a tecnologia avançada, em 2005 também alterou a forma de atuação do *phishing*:

> Após o ano 2005 os criminosos tornaram-se mais sofisticados e começaram a usar *crimeware* em conjunto com os seus *Websites* falsos e hostis tendo em vista explorar vulnerabilidades nos *browsers* para infectar os sistemas informáticos. Usando esta técnica, é feito um furto de identidade dos utilizadores não sendo sequer necessário a inserção de dados pessoais pois estes são roubados quando se acede a sítios legítimos de bancos e de outros serviços *online*.

No entanto, diante tais aspectos, faz-se necessário mais uma vez distinguir o ciberterrorismo do cibercrime. Assim, o objetivo primordial dos ciberterroristas está na difusão do pânico e do medo na sociedade. Logo, para atingir determinado fim, os vírus, trojans e o *phishing* são munições essenciais para tal ataque. Porém, tais munições sozinhas não logram êxito, devendo existir o dolo de causar danos nos sujeitos atingidos "de modo que, somente quando os vírus e demais formas, forem utilizados para causarem pânico em massa é que eles poderão ser considerados como armas do ciberterrorismo" (OLIVEIRA; SILVA, 2019). Destarte, apesar dessas formas de atuação *retro* mencionadas, deve ser apreciado o uso da *Internet* por essa particularidade de agentes, incluindo análises sobre a *Deep Web e Dark Web*, pois 99% das atividades terroristas (ALCÂNTARA, 2015) e ciberterroristas ocorrem neste nível do ciberespaço.

CONSIDERAÇÕES FINAIS

A *internet* surgiu em meados dos anos 1960, tendo sido apresentada ao Brasil a partir de 1994, introduzindo o país ao contexto tecnológico e globalizado. Concomitante ao desenvolvimento da rede no território brasileiro, os aparelhos eletrônicos adquiriram uma vasta proporção no meio da sociedade, de modo que se tornou impossível viver a mesma. É inegável que a *internet* foi uma das melhores ferramentas tecnológicas criadas, tendo em

vista como facilitou a vida humana, de forma que o ciberespaço trouxesse uma nova e aprimorada forma de vivência em sociedade. Com tamanha amplitude desse ambiente digital, além de benefícios trouxe também desvantagens, como a criação de diversos crimes e o ciberterrorismo, que ameaça e intima governos e sociedades por meio do pânico e do medo. Desse modo, o ciberterrorismo potencializa o crime de terrorismo comum, posto que se desdobra no ciberespaço, um ambiente virtual de comunicação e transmissão de dados através da interconexão global dos computadores ou qualquer outro aparelho tecnológico. Ademais, o ciberespaço não comporta fronteiras, tendo como principal característica a velocidade em que os atos circulam, diferentemente do mundo físico.

A porta de entrada para o ciberespaço é a *internet*, sendo melhor interpretada devido a *World Wide Web*, compreendendo dobras semióticas que se subdivide em três níveis: *Surface Web*, *Deep Web* e *Dark Web*, constituindo uma verdadeira complexidade, com sistemas de interação intricados e abertos, onde uma ação é capaz de gerar uma grande reação. Devido a suas vulnerabilidades, o espaço cibernético se tornou um âmbito perfeito para a prática de diversas condutas ilícitas. Nessa perspectiva, um indivíduo com um pouco de conhecimento na área de informática, é capaz de criar um *vírus* e espalhá-lo para danificar o funcionamento de diversos serviços públicos. Tais exemplos não se encontram distantes da realidade, tendo em vista o ciberataque ocorrido em 12 de maio de 2017 mediante o *malware WanaCrypt0r*.

Mesmo diante divergências entre os pesquisadores do tema, é incerto se um ataque ciberterrorista já se realizou. Contudo, diante situações hipotéticas e mediante um experimento realizado no ano de 2007 pelo Laboratório Nacional de Idaho, é perfeitamente possível arruinar uma infraestrutura de gerador de diesel através de meios cibernéticos. Da mesma forma que o terrorismo não apresenta um consenso quanto ao seu conceito, o ciberterrorismo também ostenta certas dificuldades na matéria, obstando a criação de um tipo penal específico para tal conduta. Contudo, diante inúmeras pesquisas acerca do tema, o ciberterrorismo afigura um ataque ilegal mediante o uso de aparelhos eletrônicos conectados à *Internet*, com o intuito de causar terror e graves prejuízos.

A diferença entre ciberguerra, cibercrimes e ciberterrorismo é demonstrada a partir dos seus sujeitos ativos e passivos. Na ciberguerra, a agressão cibernética é promovida de Estado para Estado, com o fim de impor seus objetivos e danificar a capacidade do outro. Os cibercrimes, ou crimes cibernéticos, são confundidos com o ciberterrorismo, portanto se difere quanto a motivação, finalidade e extensão do dano que almeja causar, tendo em

vista que o cibercrime é motivado pela obtenção de uma vantagem econômica e o ciberterrorismo não, apenas possui o dolo específico de causar um dano de grande proporção por razões políticas ou religiosas através do medo infligido. Os governos mundiais estão atentos quanto a gravidade do tema e já adequaram seus ordenamentos jurídicos para a nova realidade tecnológica. O país pioneiro a realizar alterações em sua legislação foram os EUA, devido ao ataque realizado em 11 de setembro de 2001, adotando medidas de combate ao terrorismo e ciberterrorismo no *Patriot Act*. Nesse sentido, o Reino Unido também passou a coibir e punir através de legislações severas o terrorismo e atos ciberterroristas através do *Terrorism Act* 2000, 2006 e 2008.

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

Assim, o legislador pátrio, empenhando-se a aprimorar o ordenamento jurídico no que dispõe a Constituição, bem como nivelar-se à política antiterrorista estrangeira, submeteu ao Congresso Nacional o Projeto de Lei nº 2.016/15 que se tornou a Lei Ordinária nº 13.260/2016, conhecida como Lei Antiterrorismo e apresenta características de um Direito Penal do Inimigo, uma teoria concebida por um doutrinador alemão, que traz como princípios basilares da teoria a insegurança e o medo. Assim, a Lei relativiza direitos, tendo um perfil de tutela penal punitiva e preventiva, ferindo alguns princípios constitucionais previstos.

Entretanto, apesar da Lei ter previsto de forma ínfima a conduta ciberterrorista, é meritório o avanço apresentado no ordenamento. O melhor enquadramento da conduta de ciberterrorismo é tipificado no §1º, inciso IV do artigo 2º, evidenciando o dolo específico de gerar o pânico generalizado com um rol exemplificativo. Além disso, referido artigo traz conceitos próximos dos abordados no presente trabalho, ou seja, define o ciberterrorismo pela finalidade do ato, que é intimidar ou coagir governos ou sociedades, em prol de

objetivos políticos, religiosos ou ideológicos. A primeira aplicação efetiva da Lei foi com a Operação *Hashtag*, por meio da qual foram punidos oito suspeitos por seus atos preparatórios, de um suposto ataque terrorista que iria ocorrer durante as Olímpiadas sediadas no Brasil em 2016. Por fim, é reconhecido o avanço legislativo a partir da elaboração de uma Lei Federal que tipifica condutas de terrorismo e, de forma breve, do ciberterrorismo. Contudo, críticas pairam sobre a Lei, tais como a lesão da ordem constitucional do Estado brasileiro, uma vez que afronta princípios previstos na Carta Magna, tais como isonomia e presunção de inocência, sendo defendido que não deve haver um Direito Penal para cidadãos e outro excepcional para supostos inimigos. Desse modo, compreensível o entendimento de que a legislação carece de reforma, bem como de maior debate com a doutrina penalista.

REFERÊNCIAS

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

_____. Terroristas e Internet: Novas ameaças do século XXI. **Segurança internacional, estudos estratégicos e política de defesa**, Belo Horizonte-MG, 2017. Disponível em: http://www.encontro2017.abri.org.br/site/anaiscomplementares2?AREA=9#B. Acesso em: 20 ago. 2019.

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

ALMEIDA, Débora de Souza de; CUNHA, Rogério Sanches. O ciberataque do dia 12 de maio: ciberterrorismo? **Meusitejurídico.com**. 16 maio. 2017. Disponível em: <https://pdfdocumento.com/ciberterrorismo-amazon-simple-storage-service-s3_59cb63161723dd07b65c80cd.html>. Acesso em: 20 ago. 2019.

AVAST. **O que é *Phishing*?**. Disponível em: https://www.avast.com/pt-br/c-phishing. Acesso em: 22 jul. 2019.

BERGMAN, Michael. White paper: the Deep Web: surfacing hidden value**. Journal of electronic publishing**. Michigan: University of Michigan Library, vol.7, Ed.1, 2001. Disponível em: <https://brightplanet.com/2012/06/18/the-deep-web-surfacing-hidden-value/>. Acesso em: 20 jul. 2019.

CALDERON, Barbara. **Deep & Dark Web**: A internet que você conhece é apenas a ponta do iceberg. Rio de Janeiro: Alta Books, 2017. 268 p.

CARTA CAPITAL. **Entenda o significado de Jihad**. Disponível em: https://www.cartacapital.com.br/blogs/dialogos-da-fe/entenda-o-significado-de-jihad/. Acesso em: 20 jul. 2019.

CARVALHO, Maximiliano Pereira de. Os ciberataques constituem uma real ameaça à justiça digital? **Revista dos Tribunais Online**, v. 119, p. 117-132, mar. 2019. Disponível em: http://revistadostribunais.com.br. Acesso em: 20 ago. 2019.

CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Tradução: Maria Luiza X. de A. Borges. 1. ed. Rio de Janeiro/RJ: Zahar, 2003. 244 p.

_____. **A Sociedade em Rede.** São Paulo: Paz & Terra, 2009. 630 p.

CHAGAS, Morgana Santos das. **Ciberterrorismo:** as possibilidades da expansão do terror nas Relações Internacionais. Monografia (Bacharelado em Relações Internacionais) - Universidade Estadual da Paraíba, João Pessoa - PB, 2013. Disponível em: http://dspace.bc.uepb.edu.br/jspui/handle/123456789/11089. Acesso em: 20 ago. 2019.

COMPUTER PORTUGUÊS. **O arranjo lógico dos nós de uma rede**. Disponível em: <http://ptcomputador.com/Networking/local-networks/71418.html>. Acesso em: 11 jul. 2019.

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

FREENET PROJECT. **What is Freenet?.** Disponível em: https://freenetproject.org/pages/about.html. Acesso em: 4 ago. 2019. (tradução nossa).

GARDINI, Mayara Gabrielli. Terrorismo no ciberespaço: o poder cibernético como ferramenta de atuação de organizações terroristas. **Fronteira**, Belo Horizonte-MG, ano 2014, v. 13, n. 25 e 26, p. 7-33, 2014. Disponível em: http://periodicos.pucminas.br/index.php/fronteira/article/view/10461. Acesso em: 20 ago. 2019.

INTERNET GOVERNANCE FORUM. **About the IGF**. Disponível em: https://www.intgovforum.org/multilingual/tags/about. Acesso em: 1 jul. 2019.

INTERNET RIGHTS AND PRINCIPLES COALITION. **The charter of Human Rights and Principles for the Internet**. Disponível em: http://internetrightsandprinciples.org/site/. Acesso em: 1 jul. 2019.

KRETSCHAMANN, Ângela; WENDT, Emerson. **Tecnologia da informação & Direito**. Porto Alegre: Livraria do Advogado, 2018. 166 p.

LÉVY, Pierre. **Cibercultura**. Tradução: Carlos Irineu da Costa. São Paulo: 34 Ltda, 1999. 272 p.

LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. **20 anos da internet no Brasil**, p. 11-45, jan./abr. 2013. Disponível em: http://aslegis.org.br/. Acesso em: 11 jul. 2019.

MARQUES, Alex Lopes; GONTIJO, Samuel Eugênio Melo. **Grupos Terroristas Islâmicos e a Internet:** Como terroristas fazem uso de cibercrime e prejudicam a imagem da população muçulmana. Disponível em: http://www.sigmadf.com.br/wp-content/uploads/sites/24/2016/06/FINAL-Artigo-CPCJC.pdf. Acesso em: 20 jul. 2019

O GLOBO. **Os oito ataques mais marcantes na ciberguerra mundial**. Disponível em: https://oglobo.globo.com/economia/os-oito-ataques-mais-marcantes-na-ciberguerra-mundial-21332519. Acesso em: 20 ago. 2019.

OLIVEIRA, Pedro Moisés Ribeiro de; SILVA, Rubens Alves da. Ciberterrorismo e o direito penal: uma análise criminológica. **Boletim Jurídico**, Uberaba/MG, a. 13, no 1647. Disponível em: <https://www.boletimjuridico.com.br/ doutrina/artigo/5116/ciberterrorismo-direito-penal-analise-criminologica> Acesso em: 14 out. 2019.

OPOVO ONLINE. **11 de setembro**: 17 curiosidades sobre o atentado às Torres Gêmeas. Disponível em: 11-de-setembro-17-curiosidades-sobre-o-atentado-as-torres-gemeas.html. Acesso em: 20 jul. 2019.

PINTO, Marco Aurélio Gonçalves. **Teoria relativista do Ciberterrorismo**. 115 p. Dissertação (Mestrado em Guerra da Informação) - Academia Militar - Departamento de estudos pós-graduados, Lisboa, 2011. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/6826/1/Ciberterrorismo_tese_VersFinal.pdf. Acesso em: 22 jul. 2019.

POMPÉO, Wagner Augusto Hundertmarck; SEEFELDT, João Pedro. Nem tudo está no Google: *Deep Web* e o perigo da invisibilidade. In: Congresso Internacional de Direito e Contemporaneidade, 2., 2013, Santa Maria. **Anais.**.. Santa Maria: Ufsm, 2013. p. 436-449. Disponível em: <http://www.coral.ufsm.br/congressodireito/anais/2013/3-11.pdf>. Acesso em: 21 jun. 2019.

Princípios para a governança e uso da Internet, 2011. Disponível em: https://principios.cgi.br/. Acesso em: 21 jun. 2019.

UNITED NATIONS SECURITY COUNCIL. **Resolution 1566 (2004)**. Disponível em: https://undocs.org/S/RES/1566(2004). Acesso em: 20 jul. 2019. (tradução nossa).

WE ARE SOCIAL. **Digital 2019:** Global Internet Use Accelerates. Inglaterra, 2019. Disponível em: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates. Acesso em: 18 jul. 2019.