

**CIBERTERRORISMO E DIREITO PENAL:
ANÁLISE DA PROPORCIONALIDADE DA LEI
Nº 13.260/2016 ENQUANTO INSTRUMENTO
DE PROTEÇÃO DO DIREITO FUNDAMENTAL
À SEGURANÇA**

*CYBERTERRORISM AND CRIMINAL LAW: ANALYSIS OF
THE PROPORTIONALITY OF LAW Nº 13.260/2016 AS AN
INSTRUMENT TO PROTECT THE FUNDAMENTAL RIGHT
TO SECURITY*

André Machado Maya¹

FMP-RS

Ariel Fraga²

FMP-RS

Resumo

O presente trabalho tem como objetivo analisar a proporcionalidade da Lei nº 13.260/2016 enquanto instrumento de proteção dos bens jurídicos expostos a risco pelo ciberterrorismo, em especial observadas as dimensões de proibição de excesso e de insuficiência do mencionado postulado normativo. A este efeito, o presente ensaio inicia por uma análise da atual sociedade de risco globalizada e influenciada pelas tecnologias da informação e comunicação, em especial a Internet. Nesse contexto é apresentado o problema do ciberterrorismo, na segunda parte do estudo, com especial ênfase à sua definição e à identificação do direito fundamental à segurança como bem jurídico exposto a risco por essa prática delituosa. Ao final, a pesquisa centra-se na verificação da ponderação do

¹ Doutor e Mestre em Ciências Criminais pela PUCRS. Especialista em Direito do Estado pela UniRitter e em Ciências Penais pela PUCRS. Professor de Direito Penal e Processo Penal dos cursos de graduação e mestrado em Direito da Fundação Escola Superior do Ministério Público do Rio Grande do Sul (FMP). Membro fundador do Instituto Brasileiro de Direito Processual Penal (IBRASPP). Advogado. E-mail: andremmaya@gmail.com.

² Cursa especialização em Direito Civil e Processo Civil pela Fundação Escola Superior do Ministério Público do Rio Grande do Sul (FMP-RS). Bacharel em Direito pela Fundação Escola Superior do Ministério Público do Rio Grande do Sul (FMP-RS). Advogado. E-mail:arielfraga1@hotmail.com

tratamento penal dispensado pela Lei nº 13.260/2016 aos atos de ciberterrorismo, culminando com a conclusão de que a legislação confere proteção insuficiente ao excluir do âmbito de proteção da norma os ataques a servidores ou redes privadas de uso individual.

Palavras chave

Ciberterrorismo. Direito Penal. Direito à segurança. Proporcionalidade. Proibição de proteção insuficiente.

Abstract

The present work aims to analyze the proportionality of Law No. 13.260/2016 while an instrument for the protection of legal goods that are exposed a risk due to cyberterrorism, especially observed as the measures to prohibit overweight and insufficient normative postulates. This effect, the present essay begins an analysis of the current globalized risk society and that is influenced information and communication technologies, in particular the Internet. In this context, the problem of cyberterrorism is presented in the second part of the study, with special emphasis on its definition and identification of the fundamental right to security as a legal good exposed to a risk for this criminal practice. In the end, the research centered on verifying the weighting of the criminal treatment given by Law No. 13.260/2016 to acts of cyberterrorism, culminating in the conclusion that the legislation provides insufficient protection by excluding attacks on servers from the scope of the rule or private networks for individual use.

Keywords

Cyberterrorism. Criminal Law. Right to security. Proportionality. Prohibition of insufficient protection.

INTRODUÇÃO

No contexto de uma sociedade de risco marcada pelo constante avanço das tecnologias de informação e comunicação, as práticas terroristas convencionais encontraram no mundo digital globalizado um ambiente propício para a propagação do medo e da insegurança. A consolidação da internet como principal instrumento de comunicação social, assim como a rápida evolução das redes de conexões, propiciam a exposição a risco de uma infinidade de bens jurídicos individuais e transindividuais, como, por exemplo, a vida, a saúde, o sistema econômico-financeiro, os dados e a própria incolumidade pública. Nesse cenário, tem sido comum o uso do Direito Penal como instrumento de controle social, em resposta às demandas por segurança formuladas pela sociedade ao Estado.

Atento a isso, o presente estudo tem como objetivo analisar a proporcionalidade da Lei nº 13.260/2016, enquanto instrumento de proteção dos bens jurídicos expostos a risco pelo ciberterrorismo, em especial do direito fundamental à segurança. O problema a que se propõe a responder pode ser sintetizado nas seguintes indagações: a criminalização do ciberterrorismo pela Lei nº 13.260/2016 é adequada e necessária à tutela do direito fundamental à segurança? Em caso afirmativo, o tratamento penal dispensado pela mencionada legislação aos atos de ciberterrorismo confere proteção adequada às proibições de excesso e de insuficiência, decorrentes do postulado normativo da proporcionalidade?

A este efeito, o ensaio está estruturado em três partes distintas. A primeira parte é destinada à contextualização da sociedade de risco globalizada e sua relação com a expansão do controle estatal pela via penal, material e adjetiva. A segunda parte possui como foco o exame da sociedade da informação e sua relação com a criminalização do ciberterrorismo, com especial ênfase na definição doutrinária dessa prática ilícita. O intuito é identificar um paralelo entre a evolução do risco (inerente ao avanço das tecnologias de informação e comunicação) e a necessidade de aprimoramento do tratamento penal destinado às práticas terroristas. Ao final, na terceira parte o presente ensaio, é analisada a Lei nº 13.260/2016, com especial ênfase à identificação do direito fundamental à segurança como bem jurídico tutelado, e então examinada a adequação, a necessidade e, com especial relevância, a razoabilidade do tratamento penal do ciberterrorismo.

A pesquisa segue metodologia dedutiva e centra-se na técnica de revisão bibliográfica e análise legislativa e doutrinária sobre tema atual e relevante para as ciências criminais.

1. A SOCIEDADE DE RISCO E A EXPANSÃO DO CONTROLE ESTATAL PELA VIA PENAL

A ideia de sociedade de risco surge, com essa denominação, no escrito do sociólogo alemão Ulrich Beck,³ em 1986. Com o objetivo de explicar questões relacionadas àquele estágio da modernidade, o autor associou a produção de riqueza à produção social de riscos, como característica do que denominou de modernidade tardia. Aos problemas e conflitos distributivos da sociedade da escassez, sobrepõem-se os problemas e conflitos surgidos a partir da produção, definição e distribuição de riscos científicos tecnologicamente alcançados. A teoria de Beck está estruturada nas diferenças entre a sociedade industrial e a chamada modernidade tardia, em especial identificadas pela produção do risco e pelas formas como esses riscos afetavam as relações sociais, políticas e econômicas do final do Século XX.

Nessa linha, se estrutura a ideia de que modernidade reduz o risco geral de determinadas áreas e modos de vida, mas simultaneamente cria novos riscos, pouco conhecidos ou inteiramente desconhecidos em períodos anteriores. Esses parâmetros incluem riscos de alta consequência, derivados do caráter globalizado dos sistemas sociais da modernidade. O mundo moderno tardio — chamado de alta modernidade por Giddens⁴ — é apocalíptico não porque se encaminha inevitavelmente à calamidade, mas porque introduz riscos que gerações anteriores não tiveram que enfrentar. Assim, por exemplo, por mais que tenha havido progresso na negociação internacional e no controle das armas, enquanto continuarem a existir armas nucleares, ou mesmo o conhecimento necessário para a sua construção, e uma vez que a ciência e a tecnologia continuem sendo utilizadas para a criação de

³ BECK, Ulrich. *Sociedade de Risco: rumo a uma outra sociedade*. Tradução: Sebastião Nascimento. 2. Ed. São Paulo: Editora 34, 2011, p. 23.

⁴ GIDDENS, Anthony. *Modernidade e identidade*. Tradução: Plínio Dentzien. Rio de Janeiro: Editora Zahar, 2002, p. 11. Base de Dados Minha Biblioteca.

novos armamentos, o risco da guerra maciçamente destrutiva permanecerá.

Conforme Guzella⁵, as novas tecnologias, aliadas ao notável desenvolvimento de diversas áreas do conhecimento humano, criam novas situações que exigem maior proteção e segurança aos indivíduos, num processo contínuo, despercebido e praticamente independente de mudanças que afetam as bases da sociedade industrial. Dessa forma, diante de uma realidade em contínua mutação, as pessoas tendem a valorizar as antigas certezas da sociedade industrial, criando momentos em que se faz necessário decidir entre uma convicção do passado e uma realidade transformadora.

O processo de modernização, então, torna-se “reflexivo”, convertendo-se a si mesmo em tema e problema. Às temáticas do desenvolvimento e do emprego de tecnologias – no plano da natureza, sociedade e personalidade – se sobrepõem questões referentes ao seu uso político e científico, como administração, descoberta, integração, prevenção e acobertamento dos riscos de tecnologias efetivas ou potencialmente empregáveis. Com isso, a promessa de segurança avança com os riscos, em muitos casos exposta ao debate público.⁶

Os riscos e ameaças de hoje são diferentes dos seus equivalentes passados, fundamentalmente por consequência da globalidade de seu alcance e de suas causas modernas. São riscos decorrentes da própria modernização, um produto de série do maquinário industrial do progresso, que é sistematicamente agravado com desenvolvimento ulterior.⁷

⁵ GUZELLA, Thatiana Laiz. *A expansão do direito penal e a sociedade de risco*. Publica Direito. Brasília, Distrito Federal, nov. 2008, p. 3073. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/brasilia/13_357.pdf. Acesso em: 14 abr. 2019.

⁶ BECK, Ulrich. *Sociedade de Risco: rumo a uma outra sociedade*. Tradução: Sebastião Nascimento. 2. Ed. São Paulo: Editora 34, 2011, p. 24.

⁷ BECK, Ulrich. *Sociedade de Risco: rumo a uma outra sociedade*. Tradução: Sebastião Nascimento. 2. Ed. São Paulo: Editora 34, 2011, p. 26.

Uma das características mais evidentes que aparta a chamada modernidade tardia de qualquer período anterior é seu extremo dinamismo. O mundo contemporâneo é um “mundo em disparada”. Não só o ritmo da mudança social é muito mais acelerado que em qualquer sistema anterior; como também a amplitude e a profundidade com que ela afeta práticas sociais e modos de comportamento preexistentes são maiores.⁸

Nesse cenário, em que o desenvolvimento da ciência e da tecnologia pauta a produção de riscos e propicia o fomento da insegurança, Bauman alerta ao fato de que “a geração mais tecnologicamente equipada da história humana é aquela mais assombrada pelos sentimentos de insegurança e desamparo”.⁹ A propósito, Silva Sánchez¹⁰ define a sociedade atual como sociedade “da insegurança sentida” (ou como sociedade do medo), pois o traço mais significativo da era pós-industrial é a sensação geral de insegurança, do que resulta uma nova forma de viver os riscos. Daí o crescimento das demandas por segurança direcionadas ao Estado, a quem compete a estabilização das relações sociais, e o uso do Direito Penal “como dique de contenção às novas problemáticas”.¹¹

A par disso, o surgimento de novas áreas de interesse social, como a genética, o meio ambiente, a economia e a informática, normalmente associadas ao fenômeno da globalização e da transnacionalização dos fatos sociais, acabam, de acordo com D’Ávila, criando novos espaços de regulamentação jurídica, para os

⁸ GIDDENS, Anthony. *Modernidade e identidade*. Tradução: Plínio Dentzien. Rio de Janeiro: Editora Zahar, 2002, p. 21. Base de Dados Minha Biblioteca.

⁹ BAUMAN, Zygmunt. *Medo Líquido*. Tradução: Carlos Alberto Medeiros. 1. Ed. Rio de Janeiro: Editora Zahar, 2008, p. 132.

¹⁰ SILVA SÁNCHEZ, Jesús María. *A expansão do direito penal: aspectos da política criminal nas sociedades pós industriais*. Tradução: Luiz Otávio de Oliveira Rocha. – São Paulo: Editora Revista dos Tribunais, 2002.(Série as ciências criminais no século XXI, v.11), p. 33.

¹¹ GUZELLA, Thatiana Laiz. *A expansão do direito penal e a sociedade de risco*. Publica Direito. Brasília, Distrito Federal, nov. 2008, p. 3071. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/brasil/13_357.pdf. Acesso em: 14 abr. 2019.

quais o Estado se vale também do Direito Penal como instrumento de controle. Neste contexto ocorre uma natural expansão quantitativa e qualitativa do Direito Penal.¹²

Assim, o ramo do Direito que historicamente era considerado a última alternativa para o enfrentamento de violações ao sistema jurídico passa a assumir um caráter de *prima ratio*, como responsável pela estabilização das relações sociais e pela redução dos riscos ou das suas potencialidades lesivas.¹³ É nesse contexto que a expansão do direito penal, identificada por Silva Sanchez, caminha no sentido da prevenção de danos, da neutralização dos riscos, e disso decorre o incremento dos tipos penais de perigo – concreto e abstrato – e a criminalização de atos preparatórios, por exemplo.¹⁴

Especificamente em relação à criminalidade relacionada com a tecnologia, Silva Sanchez pontua que o desenvolvimento tecnológico abre espaços para a mutação da delinquência dolosa, proporcionando o surgimento de condutas delitivas que se projetam a partir dele. Exemplo disso é o desenvolvimento das novas formas de criminalidade organizada, que acabam por operar em nível internacional e constituem claramente um dos novos – e mais significativos – riscos para os indivíduos e os Estados.¹⁵

¹² D'ÁVILA, Fábio Roberto. Liberdade e segurança em direito penal. O problema da expansão da intervenção penal. *Revista Eletrônica de Direito Penal*. Ano 1, vol. 1, nº 1, jun. 2013, p. 66. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/redpenal/article/view/7142/5118>. Acesso em: 29 abr. 2019.

¹³ LEAL, Rogério Gesta. *A responsabilidade penal do patrimônio ilícito como ferramenta de enfrentamento da criminalidade*. E-book. Fundação Escola Superior do Ministério Público, Porto Alegre, 2017, p. 119-120. Disponível em: https://www.fmp.edu.br/wp-content/uploads/2017/10/responsabilidadepenal_EBOOK.pdf. Acesso em 29 abr. 2019.

¹⁴ MAYA, André Machado. *O processo penal na sociedade de risco: a persecução penal no Brasil entre os ideais de liberdade e segurança*. *Revista de Estudos Criminais*, ano 2019, v. 18, nº 73, p. 179-219.

¹⁵ SILVA SÁNCHEZ, Jesús María. *A expansão do direito penal: aspectos da política criminal nas sociedades pós industriais*. Tradução: Luiz Otávio de Oliveira

Esses riscos inerentes à sociedade contemporânea não representam catástrofes, mas geram instabilidade à ordem democrática.¹⁶ Daí a importância da compreensão crítica acerca dos efeitos da sociedade de risco globalizada no âmbito do Direito Penal e do Processo Penal, de modo a minimizar expansionismos normativos que restrinjam indevidamente garantias imprescindíveis à estruturação democrática do Direito Penal e do Processo Penal. O uso do Direito Penal como instrumento de controle dos riscos próprios da atual formatação social deve ser restrito ao estritamente necessário, como instrumento efetivamente de *ultima ratio* na tutela de bens jurídicos relevantes para a atual quadra histórica.

Mas ainda que assentada essa premissa, que de longe é objeto de consenso no âmbito da política criminal, certo é que a abertura tecnológica percebida nas últimas duas décadas potencializou as instabilidades inerentes à sociedade de risco globalizada. A dinâmica atual, pautada na instantaneidade da informação por intermédio da tecnologia, é o novo ingrediente a ser considerado neste cenário de instabilidades e no dimensionamento do uso do direito penal como instrumento de controle social. A esse aspecto é destinado o tópico seguinte.

2. A SOCIEDADE DA INFORMAÇÃO E A CRIMINALIZAÇÃO DO CIBERTERRORISMO

Devido à penetrabilidade em todas as esferas da atividade humana, a revolução da tecnologia da informação se impõe como ponto central de análise da complexidade da nova

Rocha. – São Paulo: Editora Revista dos Tribunais, 2002.(Série as ciências criminais no século XXI, v.11), p. 30.

¹⁶ LEAL, Rogério Gesta. *A responsabilidade penal do patrimônio ilícito como ferramenta de enfrentamento da criminalidade*. E-book. Fundação Escola Superior do Ministério Público, Porto Alegre, 2017, p. 57-58. Disponível em: https://www.fmp.edu.br/wp-content/uploads/2017/10/responsabilidadepenal_EBOOK.pdf. Acesso em 29 abr. 2019.

sociedade, sua economia e cultura em desenvolvimento. A tecnologia não determina a sociedade, nem a sociedade escreve o curso de transformação da tecnologia, uma vez que vários fatores – inclusive a criatividade e iniciativa de empreendedores – intervêm no processo de descoberta científica, inovações tecnológicas e conseqüentemente a sua aplicação no âmbito social.¹⁷ No entanto, a revolução tecnológica que caracteriza a sociedade de risco globalizada propicia uma nova dinâmica do fluxo de informação, o que, inequivocamente, é determinante para a formatação social.

A expressão “sociedade da informação”, segundo Werthein¹⁸, começou a ser utilizada nos últimos anos como substituto para o complexo conceito de “sociedade pós-industrial” e como maneira de transmitir o conteúdo específico do “novo paradigma técnico-econômico”. Portanto, a realidade que os conceitos das ciências sociais procuraram revelar refere-se às transformações técnicas, organizacionais e administrativas que têm como “fator-chave” não mais os elementos baratos da energia – como na sociedade industrial – mas os elementos baratos de informação possibilitados pelos avanços tecnológicos na microeletrônica e telecomunicações.

Consoante Gouveia¹⁹, a sociedade da informação está fundamentada nas tecnologias que englobam a aquisição, o armazenamento, o processamento e a distribuição de informação por meios eletrônicos, como rádio, televisão, telefone, computadores, entre outros. No mesmo sentido de Castells,

¹⁷ CASTELLS, Manuel. *A sociedade em rede*. Tradução: Roneide Venâncio Majer; atualização para a 6ª edição: Jussara Simões - (A era da informação: economia, sociedade e cultura; v.1) São Paulo: Ed. Paz e Terra, 1999, p. 43.

¹⁸ WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Revista Ciência da Informação* - Ci. Inf., Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000, p. 71. Disponível em: <http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf>. Acesso em: 05 maio de 2019.

¹⁹ GOUVEIA, Luis Manoel Borges. *Sociedade da informação*: Notas de contribuição para uma definição operacional. Universidade Fernando Pessoa, Portugal, 2004, p. 1. Disponível em: http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf. Acesso em: 05 maio de 2019.

assevera que estas tecnologias não transformam a sociedade por si só, mas são empregadas pelas pessoas em seus contextos sociais, econômicos e políticos, surgindo daí uma nova comunidade em âmbito local e global, denominada de “sociedade da informação”.

De acordo com Takashi²⁰, o trajeto rumo à sociedade da informação é repleto de desafios em todos os países do globo. Entretanto, em cada um, o desafio reflete uma combinação especial de oportunidades e de riscos. Assim, todos os países caminham, voluntária ou involuntariamente, rumo à sociedade da informação, competindo a cada um definir suas rotas e prioridades. Os caminhos conhecidos, no entanto, passam invariavelmente pelas técnicas relacionadas ao desenvolvimento de computadores, processamento de dados e internet.

Para Capobianco²¹, o desenvolvimento tecnológico e científico, que foi acelerado por ocasião da Segunda Guerra Mundial, permitiu a integração das potencialidades de recursos que resultaram na internet, que pode ser conceituada como uma estrutura global que encadeia os computadores e outros equipamentos para possibilitar o registro, produção, transmissão e recepção de informações e a comunicação entre indivíduos independente da sua posição geográfica.

Sendo assim, hoje resta claro que a espécie humana alcançou uma fase evolutiva inédita na qual os aspectos intelectuais e de relações da convivência dos sujeitos sofrem metamorfoses com uma rapidez nunca antes experimentada. Isso se deve em parte à função mediadora, quase onipresente, dessas novas tecnologias. Porém, acompanhando as enormes oportunidades de incremento

²⁰ TAKASHI, Tadao (Org.). *Sociedade da Informação no Brasil*: Livro Verde. Ministério da Ciência e Tecnologia, Brasília, 2000, p. 11. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/livroverde.pdf>. Acesso em: 07 maio de 2019.

²¹ CAPOBIANCO, Ligia. A Revolução em Curso: Internet, Sociedade da Informação e Cibercultura. *Revista de Estudos em Comunicação*, nº 7 - Volume 2, 175-193, Maio de 2010, p. 175. Disponível em: <http://www.ec.ubi.pt/ec/07/vol2/EC07-2010-vol2.pdf>. Acesso em: 09 de maio de 2019.

da sociabilidade humana, surgem também novos riscos, bem como discriminação e desumanização.²²

A globalização – com a facilidade de comunicação que lhe é inerente – permitiu o florescimento de campanhas altruístas de efetivação de direitos civis e de questões ambientais – salvar o planeta e os animais –, por exemplo, mas na mesma medida viabilizou, também, a estruturação de organizações criminosas dedicadas as mais variadas áreas de atuação²³ – desde a venda ilícita de armas, de drogas, de órgãos, até a prática do terrorismo.

Portanto, deve-se ter em mente que como qualquer outro meio, o uso disseminado da internet, mesmo em ambientes razoavelmente estáveis e seguros, apresenta riscos das mais variadas categorias.²⁴ É neste cenário, digital/informático, que a prática do terrorismo se potencializa, expandindo seu repertório como qualquer outra atividade e encontrando vantagens até então desconhecidas.

A recenticidade dessa relação entre terrorismo e internet impõe dificuldades para a definição de um conceito preciso de ciberterrorismo, o que impõe complicações para a implementação de medidas preventivas e repressivas.²⁵ Não obstante isso, é possível definir minimamente o ciberterrorismo como sendo a prática de conduta terroristas por intermédio da internet.

²² ASSMANN, Hugo. A metamorfose do aprender na sociedade da informação. *Revista Ciência da Informação - Ci. Inf.*, Brasília, v. 29, n. 2, p. 7-15, maio/ago. 2000, p. 7. Disponível em: <http://www.scielo.br/pdf/ci/v29n2/a02v29n2>. Acesso em: 07 maio de 2019.

²³ MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth. *Cyberterrorismo: a nova era da criminalidade* [Coleção Cybercrimes] – 1 reimp. Belo Horizonte: Editora D'Plácido, 2018, p. 25.

²⁴ MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth. *Cyberterrorismo: a nova era da criminalidade* [Coleção Cybercrimes] – 1 reimp. Belo Horizonte: Editora D'Plácido, 2018, p. 25.

²⁵ GORDON, Sarah; FORD, Richard. *Cyberterrorism?*. *Computers & Security*, [S.l.] v. 21, Issue 7, p. 636-647, nov. 2002, p. 3, tradução nossa.

Neste sentido, Denning²⁶, o define a partir da convergência entre terrorismo e ciberespaço, como ataques ilegais ou ameaças de ataques contra computadores, redes e as informações contidas neles quando feitas para coagir ou intimidar um governo ou seu povo em benefício de objetivos políticos ou sociais. Ainda de acordo com a autora, a qualificação do ataque como ciberterrorista pressupõe que dele resulte violência contra pessoas ou propriedade, ou pelo menos dano suficiente a produzir medo. Semelhante concepção é definida por Flor²⁷, para quem o ciberterrorismo se insere em um contexto no mundo globalizado e, em que pese o fenômeno não reste bem definido, ele representa um dos resultados do desenvolvimento tecnológico.

Na mesma linha, Falcão Júnior e Buffon²⁸, na tentativa de definir um conceito, concentram atenção no uso dos equipamentos da informática e tecnologia da informação para o cometimento de atos danosos, visando provocar o terror social ou generalizado. Já Hardy e Williams²⁹ definem o ciberterrorismo como a expressão utilizada para retratar ataques terroristas executados via Internet com o propósito de causar graves

²⁶ DENNING, Dorothy Elizabeth. *Cyberterrorism*. Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 Maio 2000, tradução nossa. Disponível em: <https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm>. Acesso em: 28 fev. 2019.

²⁷ FLOR, Roberto. Perspectiva para novos modelos de "investigação tecnológica" e proteção de direitos fundamentais na era da internet o chamado "ciberterrorismo" como um primordial exemplo, em conjunto a problemas de definição e a luta contra terrorismo e os crimes cibernéticos. *Revista dos Tribunais. Revista Brasileira de Ciências Criminais*: RBCCrim, v. 20, n. 99, p. 69-100, nov./dez. 2012, p. 2.

²⁸ FALCÃO JÚNIOR, Alfredo Carlos Gonzaga; BUFFON, Jaqueline Ana. Ciberterrorismo: entre a prevenção e o combate. In: SILVA, Angelo Roberto Ilha da (org.). *Crimes cibernéticos*. 2.ed. Porto Alegre: Editora Livraria do Advogado, 2018, p. 157.

²⁹ HARDY, Keiran; WILLIAMS, George. What is "Cyberterrorism"? Computer and Internet Technology in Legal Definitions of Terrorism. In: CHEN, Thomas e alt. *Cyberterrorism, Understanding, Assessment, and Response*. London: Springer, 2014, p. 1-24.

instabilidades, prejudicar serviços fundamentais e interferir no dia a dia da ordem econômica e social, em nome de determinada visão de mundo.

Não fugindo do entendimento dos autores acima citados, Magalhães e Sydow³⁰ sustentam que “o ciberterrorismo é o terrorismo praticado com ferramentas cibernéticas e, portanto, é delito que possui como meio necessário o meio informático, sendo tipo de forma vinculada”.

Com efeito, era inevitável que uma nova maneira de praticar atos de terror surgisse nesse contexto de globalização tecnológica. As vantagens apresentadas pelos meios digitais germinam um âmbito favorável e confortável para a prática das condutas terroristas neste ambiente, em especial pelas facilidades de ocultação da autoria e pela potencialização dos danos causados.

A par disso, o advento da Internet trouxe mudanças em vários aspectos na vida das pessoas, sendo hoje um instrumento indispensável para a convivência humana. Nesse cenário, o risco inerente ao ciberterrorismo se acentua na exata proporção da dependência da sociedade moderna para com as tecnologias e a Internet. De acordo com Magalhães e Sydow³¹, “as hipóteses de danos cibernéticos aumentam na medida em que mais áreas passam a ser controladas por sistemas informatizados”.

Nesta linha, o ciberterrorismo tem sido apontado como a nova ameaça contemporânea, apta a provocar os mesmos efeitos dos atos terroristas “tradicionais”. Assim essa nova modalidade de terror tem sido tratada pelos órgãos de segurança de Israel, os quais consideram que o fenômeno engloba as seguintes vertentes de atuação³²:

³⁰ MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth. *Cyberterrorismo: a nova era da criminalidade* [Coleção Cybercrimes] – 1 reimp. Belo Horizonte: Editora D’Plácido, 2018, p. 41.

³¹ MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth. *Cyberterrorismo: a nova era da criminalidade* [Coleção Cybercrimes] – 1 reimp. Belo Horizonte: Editora D’Plácido, 2018, p. 37.

³² COSTA, Alan Denilson Lima. Ciberterrorismo. In: VASCONCELOS, Carlos Eduardo de Oliveira (org.). *Terrorismo e outras situações de emergência*. Teoria e

O uso da Internet para realizar o recrutamento, proselitismo, angariar fundos, incitar o ódio e a violência, treinamento, inteligência e operação psicológica; a Jihad Eletrônica, representada pelos “cyberarmy” e os “electronic army”, que utilizam o espaço cibernético para realizar ataques cibernéticos e [desenvolver] as suas capacidades defensivas; e a associação de grupos terroristas clássicos com o crime organizado na Internet (cibercrime), aprendendo suas técnicas e contratando seus serviços.³³

Nesse passo, é possível identificar certos padrões presentes em grande parte das definições de ciberterrorismo. Primeiro, a essencialidade do uso dos meios da tecnologia da comunicação e informação para a sua prática, sendo justamente isso o que lhe diferencia de um ato terrorista convencional. Segundo, o escopo de gerar danos ou, ao menos, a ameaça de fazê-los por intermédio da internet ou da tecnologia. E terceiro, a finalidade de gerar terror na sociedade. Esse último ponto, relacionado aos objetivos, é justamente o que diferencia o ciberterrorismo dos demais ataques informáticos: nem todo ataque via internet é um atentado ciberterrorista.

A diferenciação é relevante, na medida em que o vasto repertório dos meios de comunicação atualmente existentes

prática da prevenção e do combate. Escola Superior do Ministério Público da União – ESMPU, 2018, p. 171-172. Disponível em: http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Biblioteca_Virtual/Livros_Digitais/ESMPU%203422_EBOOK%2BTERRORISMO.pdf. Acesso em: 03 jun. 2019.

³³ COSTA, Alan Denilson Lima. Ciberterrorismo. In: VASCONCELOS, Carlos Eduardo de Oliveira (org.). *Terrorismo e outras situações de emergência*. Teoria e prática da prevenção e do combate. Escola Superior do Ministério Público da União – ESMPU, 2018, p. 171-172. Disponível em: http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Biblioteca_Virtual/Livros_Digitais/ESMPU%203422_EBOOK%2BTERRORISMO.pdf. Acesso em: 03 jun. 2019.

possibilita o uso do computador como ferramenta para inúmeras práticas delituosas. Exemplos corriqueiros são o roubo de identidade, os vírus de computador, a prática de *hacking*, o uso de malware³⁴, a destruição ou manipulação de dados. Não obstante isso, a classificação dessas práticas como atos de ciberterrorismo depende da finalidade de gerar terror ou disseminar medo por intermédio de danos ou ameaças. É a combinação desse objetivo com o recurso aos meios eletrônicos, tendo o computador como alvo, que forma a imagem conceitual do ciberterrorismo.³⁵

Nesse cenário, ainda que as práticas terroristas tradicionais continuem a existir, certo é que, na atual formatação da sociedade contemporânea, passam a coexistir com os ataques praticados no “ciberespaço”. A guerra cibernética, assim compreendida por Kalac, é direcionada para a informação e os sistemas de informação que dão suporte às estruturas civis e militares dos países. É considerada mais sutil do que os ataques físicos e a destruição ou os atos sobre o fluxo de informações em rede e a sua manipulação (interrompendo, mudando, adicionando, etc). Estas atividades são primariamente voltadas para as informações, que são cruciais para o funcionamento dos sistemas civil e militar, como o controle aéreo, bolsa de valores e transações financeiras internacionais, por exemplo.³⁶

Assim, ataques cibernéticos em larga escala possuem o potencial de gerar um caos significativo no atual mundo contemporâneo, bem como um descontrole na vida diária das

³⁴ Códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. CARTILHA DE SEGURANÇA PARA INTERNET. *Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – Cet.br*. Disponível em: <https://cartilha.cert.br/malware/>. Acesso em: 4 jun. 2019.

³⁵ GORDON, Sarah; FORD, Richard. *Cyberterrorism?*. *Computers & Security*, [S.l.] v. 21, Issue 7, p. 636-647, nov. 2002, p. 7, tradução nossa.

³⁶ KALAC, Jasmin. *Cyber-terrorism as a threat to national security*. *International Refereed Scientific Journal Vision*, Volume 2, Issue 2, September 2017, p. 119-127, p. 120, tradução nossa. Disponível em: http://visionjournal.edu.mk/wp-content/uploads/2018/03/irsjv_v2i2_jasmin.pdf. Acesso em: 04 jun. 2019.

pessoas, que são extremamente dependentes da tecnologia da informação. As ações causadas por *hackers* podem causar caos e anarquia por meio de ataques a bancos e da paralisação total ou parcial da vida nos grandes centros urbanos dos países.³⁷ Como consequência, a sociedade começa, ainda que de maneira singela, a dar mais valor a ataques contra o seu “bem-estar virtual”, tal como o faz em relação a ataques contra a saúde física e patrimonial.³⁸

Enfim, essa “evolução” do terrorismo expõe uma das faces perversas da globalização da sociedade de risco. No entanto, como pontua Kalac, é também o seu “filho travesso”, que ameaça perigosamente as comunicações na esfera civil e militar, cuidados médicos de emergência, sistemas de tráfego de diferentes tipos, telecomunicações e outros bens.³⁹ Trata-se do efeito colateral que, lenta e inescapavelmente, vai usurpando os efeitos benéficos do medicamento. Alguns desses efeitos colaterais têm sido combatidos por intermédio do Direito Penal. O ciberterrorismo é um deles, ao qual foi dedicada a Lei nº 13.260/16, objeto da parte final do desenvolvimento do presente estudo.

³⁷ KALAC, Jasmin. Cyber-terrorism as a threat to national security. *International Refereed Scientific Journal Vision*, Volume 2, Issue 2, September 2017, p. 119-127, p. 121, tradução nossa. Disponível em: http://visionjournal.edu.mk/wp-content/uploads/2018/03/irsjv_v2i2_jasmin.pdf. Acesso em: 04 jun. 2019.

³⁸ TALIHÄRM, Anna-Maria. Cyberterrorism: in Theory or in Practice? *In: Defense Against Terrorism Review*. Vol.3, Nº 2, Fall 2010, p. 59-74, p. 69, tradução nossa. Disponível em: http://www.coedat.nato.int/publication/datr/volume6/05-Cyberterrorism_in_Theory_or_in_Practice.pdf. Acesso em: 07 jun. 2019.

³⁹ KALAC, Jasmin. Cyber-terrorism as a threat to national security. *International Refereed Scientific Journal Vision*, Volume 2, Issue 2, September 2017, p. 119-127, p. 121, tradução nossa. Disponível em: http://visionjournal.edu.mk/wp-content/uploads/2018/03/irsjv_v2i2_jasmin.pdf. Acesso em: 04 jun. 2019.

3. **Análise da Lei nº 13.260/16: o tratamento penal do ciberterrorismo enquanto materialização do direito fundamental à segurança.**

No cenário até o momento delineado, de uma sociedade de risco globalizada e pautada na aceleração da informação, dependente da internet e dos recursos tecnológicos, a prevenção de atos de ciberterrorismo está diretamente relacionada com o direito fundamental à segurança, enunciado no *caput* do artigo 5º da Constituição Federal.

Não há consenso na doutrina quanto à natureza fundamental do direito à segurança, assim como ainda carece de maior precisão o seu significado. Alessandro Barata⁴⁰ entende o direito à segurança como um direito de segunda grandeza, sem conteúdo próprio, mas relacionado à concretização e efetividade dos demais direitos fundamentais. Na mesma linha, Rafaelle de Giorgi⁴¹ critica o posicionamento da segurança como um direito fundamental, em contraposição ao risco que caracteriza a sociedade contemporânea. De acordo com o autor, a segurança não se contrapõe ao risco, mas ao perigo, motivo pelo qual uma sociedade estruturada em um direito fundamental à segurança estaria fadada ao insucesso.

Não obstante a relevância dos pesquisadores citados, a Constituição Federal brasileira prevê, formalmente, o direito à segurança como um direito fundamental.⁴² Há previsão expressa

⁴⁰ BARATTA, Alessandro. Seguridad. In: *Criminología y sistema penal* (compilación in memoriam). Editorial BdeF: Buenos Aires, 2004, p. 199-220.

⁴¹ DE GIORGI, Raffaele. The risk of risk society and the limits of law. In: *Direito Fundamental à Segurança e Direitos de Liberdade: a complexa harmonia em matéria penal* [recurso eletrônico]. MAYA, André Machado; LORENZONI, Pietro Cardia (Orgs). Págs. 39-50. Porto Alegre: FMP, 2019.

⁴² A propósito, ver: MAYA, André Machado; LORENZONI, Pietro Cardia. Direito (fundamental) à segurança? Uma aproximação a partir da jurisprudência do Tribunal Constitucional brasileiro e da Corte Interamericana de Direitos Humanos. In: *O direito penal e o processo penal como instrumentos de defesa de direitos públicos incondicionados: perspectivas brasileiras e chilenas* [recurso eletrônico]. LEAL, Rogério Gesta, sbardelotto,

nesse sentido nos artigos 5º e 6º da Carta Constitucional. Para além disso, em uma perspectiva material, sua natureza fundamental decorre da sua universalidade, moralidade e preferencialidade. Essas as características que, segundo Alexy,⁴³ quando associadas ao fato de tratarem de carências e interesses que devem ser protegidos e fomentados pelo ordenamento jurídico, caracterizam determinado direito como fundamental.

Consoante lição de Souza Neto⁴⁴, a positivação do direito fundamental à segurança no Brasil lhe confere uma perspectiva multidimensional, posto que especificado em diversas normas previstas explicita e implicitamente na Constituição Federal. As normas originadas do direito à segurança, segundo o autor, podem ser enquadradas em três dimensões, quais sejam: de estabilidade, de previsibilidade e de ausência de perigos. Aquela relacionada com a estabilidade das relações jurídicas, se materializa nas garantias da do direito adquirido, do ato jurídico perfeito e da coisa julgada; essa relacionada com a ausência de surpresas no atinente à atuação estatal, se materializa especialmente na garantia de legalidade; e esta relacionada a uma perspectiva social, da qual resultam imposições a que o Estado assegure minimamente as condições inerentes à dignidade da pessoa humana, no que se pode destacar a segurança pública.

Dessa terceira dimensão do direito à segurança decorre o papel positivo do Estado, tanto relacionado à diminuição de riscos da segurança externa –ameaças vindas do estrangeiro – como da segurança interna, em relação a ameaças que estão dentro do território nacional. Trata-se de proteção no sentido objetivo, de riscos e perigos efetivos a bens jurídicos relacionados à dignidade

Fábio Roque; ÁLVARES, Rodrigo Ríos (Orgs.). Págs. 239-266. Porto Alegre: FMP, 2019.

⁴³ ALEXY, Robert. *Constitucionalismo Discursivo*. 4.ed. Trad. Luís Afonso Heck. Porto Alegre: Livraria do Advogado, 2015.

⁴⁴ SOUZA NETO, Cádido Pereira de. Comentários ao artigo 5º da Constituição Federal brasileira. In: CANOTILHO, J.J. Gomes; SARLET, Ingo Wolfgang, STRECK, Lenio Luiz, MENDES, Gilmar Ferreira (Orgs). *Comentários à Constituição Federal brasileira*. São Paulo: Saraiva/Almedina, 2013, p. 486.

da pessoa humana; um direito à segurança de bens jurídicos.⁴⁵ Nessa perspectiva, o direito à segurança se materializa na forma de uma liberdade positiva, por intermédio da natureza objetiva dos direitos fundamentais, como um mandamento constitucional orientado ao Estado, para que concretize o conjunto de direitos fundamentais que asseguram aos cidadãos a condição de sujeitos de direitos.

Neste cenário, então, é possível compreender o tratamento penal dos atos terroristas enquanto uma materialização do direito fundamental à segurança. Com efeito, como destacado no item anterior, ainda que de maneira incipiente, o ciberterrorismo tem sido definido como a prática de atos orientados à disseminação do medo por meio de recursos tecnológicos, em especial a internet. Essa especial finalidade foi destacada da definição legal de terrorismo, no *caput* do artigo 2º da Lei 13.260/16,⁴⁶ exigível igualmente para a definição do ciberterrorismo, em razão do enunciado no inciso IV do mencionado dispositivo legal, cujo texto dispõe:

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

⁴⁵ BALTAZAR JUNIOR, José Paulo. Crime Organizado e Proibição de Insuficiência. Livraria do Advogado: Porto Alegre, 2010, p. 187-188.

⁴⁶ 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.

processamento de petróleo e gás e instituições bancárias e sua rede de atendimento;

Na doutrina, Lima⁴⁷ ressalta que o ciberterrorismo consiste no uso da tecnologia da informática para produzir um estado psíquico de terror na população, o que se verifica pelo afetamento, mediante condutas pautadas por violência ou grave ameaça, de bens jurídicos fundamentais como vida, integridade física e liberdade.

A Lei 13.260/16, a propósito, já na definição do que seja ato terrorista, deixou expressos os bens jurídicos afetados por essas condutas: pessoa, patrimônio, paz pública e incolumidade pública. Disso não deve resultar a açodada conclusão de que unicamente esses bens jurídicos são afetados por atos terroristas. Por certo, atos terroristas podem atingir bens jurídicos diversos. Inequivocamente, porém, existe uma violação preponderante à paz pública, inerente à promoção do sentimento de pânico, medo e pavor na coletividade, que é um resultado do efeito psicológico dos atos terroristas,⁴⁸ normalmente obtido por intermédio da violação de outros bens jurídicos, como os enunciados na legislação brasileira.

Com efeito, o terror, enquanto perturbação grave gerada por um perigo imediato, por uma situação fática que amedronta, aterroriza, que causa ansiedade,⁴⁹ afeta diretamente o direito fundamental à segurança, na sua dimensão de ausência de perigos. Tanto é assim que a doutrina costuma relacionar o bem

⁴⁷ LIMA, Renato Brasileiro de. *Legislação criminal especial comentada*: volume único. 6 Ed. ver., atual e ampl. Salvador: JusPODIVM, 2018, p. 924.

⁴⁸ PONTE, Antonio Carlos da; KAZMIERCZAK, Luiz Fernando. Terrorismo: análise da lei nº 13.260/16. *Revista Jurídica ESMP-SP*, São Paulo, v.11, 2017: 132-148, p. 143. Disponível em: http://www.esmp.sp.gov.br/revista_esmp/index.php/RJESMPSP/article/download/345/172. Acesso em: 15 jun. 2019.

⁴⁹ Dicionário Michaelis. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/terror>. Acesso em 08 abr. 2019.

jurídico *paç pública*⁵⁰ com o sentimento de segurança que deve pautar o ambiente social, e a incolumidade pública⁵¹ com o perigo ou risco coletivo que mitiga a segurança e o bem-estar das pessoas. A expressa menção a esses dois bens jurídicos na definição legal de terrorismo evidencia a afetação do direito fundamental à segurança por essa prática delituosa que, no atual contexto, potencializada pelos recursos tecnológicos, incrementa sobremaneira o risco até então conhecido, inerente ao terrorismo tradicional.

Nesse cenário, portanto, afigura-se justificada a utilização do Direito Penal para a tutela dos bens jurídicos afetados, em especial o direito à segurança. Observadas as parciais do postulado da proporcionalidade, o Direito Penal é instrumento adequado à tutela dos bens jurídicos expostos a risco, assim como necessário, dada a possibilidade concreta de afetação do núcleo essencial desses bens jurídicos por atentados dessa natureza. Com efeito, o terror, como destacado, enquanto perturbação grave da tranquilidade, consiste justamente no aniquilamento da paz social, do que decorre a desordem que afeta na essência a incolumidade pública.

Por derradeiro, na análise da proporcionalidade em sentido estrito, a medida de proteção conferida pelo Direito Penal, por intermédio da Lei 13.260/16, deve ser aferida pelas perspectivas da proibição de excesso e de insuficiência. Tanto significa verificar se o tratamento penal do ciberterrorismo se afigura equilibrado, se há proporcionalidade entre os meios e os fins, o que demanda um exame comparativo entre as previsões da Lei 13.260/16 e a sua finalidade de proteção do direito fundamental à segurança. Na doutrina de Canotilho, significa verificar a justa medida da intervenção estatal.⁵²

⁵⁰ A propósito, ver: LIMA, Renato Brasileiro de. *Legislação criminal especial comentada*: volume único. 6 Ed. ver., atual e ampl. Salvador: JusPODIVM, 2018, p. 896.

⁵¹ A propósito, ver: HUNGRIA, Nélson. *Comentários ao Código Penal*. Vol. IX. Arts. 250 a 361. Revista Forense. Rio de Janeiro, 1959, p. 7-14.

⁵² CANOTILHO, Joaquim José Gomes. *Direito Constitucional e Teoria da Constituição*. 3.ed. Coimbra: Almedina, 1998, p. 264.

A iniciar pela vertente da proporcionalidade enquanto proibição de intervenção excessiva, cuja vinculação com o Direito Penal decorre da concepção liberal-iluminista desse ramo do Direito,⁵³ concebido como um instrumento de *ultima ratio* na tutela de bens jurídicos, impõe-se verificar se as previsões da Lei 13.260/16, ao pretenderem tutelar o direito fundamental à segurança, não afetam de maneira excessiva as liberdades individuais envolvidas na ponderação.

Nesse ponto, a iniciar pela perspectiva de direito material, verifica-se a criminalização dos atos de terrorismo praticados por intermédio de mecanismos cibernéticos, cominando-lhes pena de reclusão de doze a trinta anos. A sanção penal é elevada, mas em princípio razoável, se considerada a gravidade abstrata do crime em questão. A disseminação do terror por intermédio de mecanismos cibernéticos é conduta com potencial para afetar de maneira determinante a paz e a incolumidade públicas, sem prejuízo da afetação de outros bens jurídicos de natureza individual, motivo pelo qual a sanção penal cominada reflete a medida justa do desvalor da conduta. Pelos mesmos fundamentos, afigura-se razoável também a pena cominada no artigo 6º, que tipifica uma espécie de participação genérica por auxílio material no crime de terrorismo.

Na mesma linha, a punição de atos preparatório, com redução da pena em patamar inferior ao estabelecido pelo artigo 14, II, do Código Penal, como previsto no artigo 5º da Lei 13.260/16, afigura-se adequada a uma tendência de expansão qualitativa da intervenção penal do Estado, indicada pela crescente opção política-criminal de antecipação ao dano e criminalização de condutas meramente perigosas, ainda que preparatórias de outros

⁵³ SARLET, Ingo Wolfgang. Constituição, Proporcionalidade e Direito Fundamentais: o Direito Penal entre a proibição de excesso e de proteção insuficiente. *Revista Opinião Jurídica*, nº 7, 2006-01, p. 162.

delitos.⁵⁴ No específico caso do ciberterrorismo, a relevância das possíveis afetações dos bens jurídicos expostos a risco por essas condutas torna razoável essa antecipação da intervenção penal.

Na perspectiva processual penal, a Lei 13.260/16 disciplina a possibilidade de aplicação de medidas cautelares patrimoniais, limitando a atuação do juiz à iniciativa da autoridade policial ou do Ministério Público, no que se mostra adequada ao modelo acusatório. Para além disso, determina a aplicação das legislações do crime organizado e dos crimes hediondos à persecução penal de atos de terrorismo e ciberterrorismo. Também nesse ponto não se vislumbra desequilíbrio no tratamento penal. Com efeito, a gravidade abstrata das condutas tipificadas pela Lei 13.260/16 é evidentemente mais elevada do que significativa parcela dos crimes hediondos e, também, dos delitos praticados por organizações criminosas – basta uma singela comparação das penas abstratas cominadas –, de maneira que irrazoável seria dar aos atos terroristas tratamento processual penal menos severo.

De outro lado, agora na perspectiva da proporcionalidade enquanto proibição de proteção insuficiente, impõe-se analisar eventuais falhas da legislação por omissão no cumprimento do imperativo de tutela enunciado no artigo 5º, XLIII, da Constituição Federal. Aqui, a proporcionalidade está relacionada com a face objetiva dos direitos fundamentais, da qual decorre a obrigação de o Estado promover a sua proteção. Consoante destaca Sarlet,⁵⁵ com amparo na doutrina de Canaris, trata-se de controlar a legitimidade constitucional de uma determinada intervenção (no caso, penal) no âmbito de proteção de um direito fundamental.

⁵⁴ MAYA, André Machado. O processo penal na sociedade de risco: a persecução penal no Brasil entre os ideais de liberdade e segurança. *Revista de Estudos Criminais*, ano 2019, v. 18, n° 73, p. 179-219.

⁵⁵ SARLET, Ingo Wolfgang. Constituição, Proporcionalidade e Direitos Fundamentais: o Direito Penal entre a proibição de excesso e de proteção insuficiente. *Revista Opinião Jurídica*, n° 7, 2006-01, p. 181.

Neste plano, apresenta-se a indagação acerca de eventual deficiência da proteção conferida pela Lei 13.260/16. Isso, basicamente, em razão de duas circunstâncias. A primeira delas, destacada pela doutrina, referente ao zelo do legislador em excluir do âmbito de criminalização eventuais atos praticados no contexto de manifestações sociais. O parágrafo 2º do artigo 2º da Lei 13.260/16 expressamente exclui a sua incidência nos casos de condutas individuais ou coletivas de pessoas em manifestações políticas, movimentos sociais, sindicais, religiosos, de classe ou de categoria profissional, direcionados por propósitos sociais ou reivindicatórios, visando a contestar, criticar, protestar ou apoiar, com o objetivo de defender direitos, garantias e liberdades constitucionais, sem prejuízo de eventual tipificação penal contida em outra legislação.

A este respeito, Veiga explica que a legislação se mostrou ideologicamente comprometida e instrumento de proteção às manifestações sociais. Aduz que restou claro o esforço empregado pelo governo para que protestos de natureza política e de classes sociais e profissionais não fossem tratados como atos terroristas, embora muitas vezes resultem em violência e depredação. Por isso, conclui, a “definição brasileira está longe de ser adequada, uma vez que está mais comprometida com bandeiras ideológicas do que com a estrutura da realidade nacional e internacional”.⁵⁶ Em sentido oposto, Cambi e Ambrosio destacam o risco de eventuais interpretações equívocas da exceção aposta no mencionado parágrafo 2º, do que pode resultar uma ameaça para movimentos populares na defesa de direitos, garantias e liberdades constitucionais⁵⁷.

⁵⁶ VEIGA, Eduardo de Lima. *Terrorismo e direito penal do inimigo*: contornos e legitimidade à luz do direito internacional. Dissertação (Mestrado em Direito)– Programa de Pós-Graduação em Direito, Fundação Escola Superior Do Ministério Público, Porto Alegre, 2018, p. 91.

⁵⁷ CAMBI, Eduardo Augusto Salomão; AMBROSIO, Felipe Augusto Rodrigues. Lei Antiterror brasileira (l. 13.260/16): ameaça à democracia e aos direitos fundamentais. *Revista Quaestio Iuris*. vol. 10, nº. 03, Rio de Janeiro, 2017. pp. 1370-1397, p. 1377. Disponível em: <https://www.e->

A segunda das circunstâncias dignas de destaque é a exclusão, do âmbito de proteção, de servidores e computadores de natureza particular e de uso privado ou individual. Conforme o enunciado do artigo 2º, §1º, IV, da legislação em questão, não são objeto da proteção penal computadores ou servidores de uso individual.⁵⁸

A toda evidência, o risco de afetação de servidores coletivos por condutas ciberterroristas é maior em relação à possibilidade de afetação de servidores de uso individual. Não obstante isso, estes servidores compõem inequivocamente a parcela majoritária da rede de informática que mantém conectada a sociedade atual, e como tal estão igualmente sujeitos às vulnerabilidades do contorno da rede, uma vez que o problema não está em um computador ou rede em especial, mas justamente na rede compartilhada. Em princípio, portanto, não se afigura justificada a exclusão dos servidores particulares do âmbito de proteção da lei.

Neste ponto, poder-se-ia justificar essa exclusão a partir de um olhar mais amplo para o sistema penal. A existência de outros tipos penais esparsos seria suficiente à tutela penal dos servidores de uso particular? A resposta, no entanto, aponta em sentido negativo.

O Direito Penal brasileiro está estruturado em um diploma geral (Código Penal) que convive com leis esparsas, especiais, por meio das quais o Estado aprimora a tutela penal de novos bens jurídicos – cuja relevância exsurge do desenvolvimento da sociedade de risco globalizada e tecnológica, como destacado na primeira parte do presente estudo – ou de bens jurídicos já conhecidos, mas cuja necessidade de tutela penal surge em razão dos ris-

publicacoes.uerj.br/index.php/quaestioiuris/article/view/24805/25799.

Acesso em: 26 jun. 2019.

⁵⁸ PONTE, Antonio Carlos da; KAZMIERCZAK, Luiz Fernando. Terrorismo: análise da lei n° 13.260/16. *Revista Jurídica ESMP-SP*, São Paulo, v.11, 2017: 132–148, p. 145. Disponível em: http://www.esmp.sp.gov.br/revista_esmp/index.php/RJESMPSP/article/download/345/172. Acesso em: 15 jun. 2019.

cos que se apresentam na formação social contemporânea. Em qualquer das hipóteses, a forma de expansão – qualitativa e quantitativa – da tutela penal é a edição de novas leis esparsas.

No atual estado da arte da legislação penal brasileira, porém, identifica-se uma tutela muito rarefeita de bens jurídicos expostos a riscos relacionados ao desenvolvimento tecnológico. Se de um lado é certo que muitos dos denominados *cibercrimes* podem ser tratados com base na legislação penal em vigor – como são os casos de delitos contra a honra e patrimônio – de outro lado há ilícitos praticados por intermédio de sistemas de informática e da rede mundial de computadores que não encontram adequação aos crimes tipificados no Código Penal. Assim se verifica nos casos de ilícitos que afetam bens jurídicos que até o momento não justificavam uma tutela penal ou que, em razão do diminuto risco a que estavam expostos, eram tutelados como ilícitos de menor potencial ofensivo, ou, ainda, porque os tipos penais existentes prevêm formas de ofensa não relacionadas à evolução tecnológica.

A Lei 12.737/12, atenta a esse cenário, introduziu no Código Penal dois tipos relacionados a condutas praticadas por intermédio da internet: invasão de dispositivo informático (artigo 154-A) e interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (artigo 266). Aquele é crime contra a liberdade individual, posto que inserido no capítulo que trata dos crimes contra a liberdade individual, e tipifica a conduta de “invadir dispositivo informático alheio, conectado ou não à rede de computadores, 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 ou instalar vulnerabilidades para obter vantagem ilícita”; este é crime contra a segurança dos meios de comunicação e transporte e outros serviços públicos, e tipifica a conduta de “interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento”.

O crime de invasão de dispositivo informático tutela a liberdade individual do proprietário do dispositivo, e indiretamente

a privacidade dos dados nele armazenados. Trata-se de previsão legal diretamente relacionada com as condutas de *hackers*, cuja origem ficou notoriamente atrelada à subtração de arquivos privados de famosa atriz brasileira. Portanto, a tutela é de bem jurídico individual. Ainda que o tipo penal possa incidir na hipótese de invasão de um número indeterminado de dispositivos, inequívoco é que basta a invasão de um único para a consumação do crime. E a sanção penal cominada (03 meses a 1 ano) a toda evidência, é diminuta e insuficiente à prevenção geral da conduta, se pensada sob a ótica da invasão de um número significativo de computadores.

O tipo penal de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, tutela a liberdade de comunicação, bem jurídico relacionado com a incolumidade pública. A propósito, o artigo 266 integra o Título dos crimes contra a incolumidade pública no Código Penal. E efetivamente, a interrupção ou a perturbação de serviços de comunicação, na atual sociedade da informação, são fatos geradores de instabilidade social. Sob este aspecto, esse tipo penal está relacionado à promoção da segurança pública na sua perspectiva social, enquanto direito à ausência de perigos. Não obstante isso, à consumação do crime basta a interrupção ou a perturbação desses serviços, sem a necessidade do intuito específico de causar medo ou terror, e sem a necessidade de que o *modus operandi* envolva violência ou grave ameaça. Além disso, a sanção penal cominada no preceito secundário do artigo 266 é também ínfima, se relacionada à gravidade abstrata das condutas ciberterroristas.

Destarte, são poucos os tipos penais especificamente relacionados a condutas ilícitas relacionadas com a tecnologia da comunicação. Ademais, esses poucos tipos tutelam outros bens jurídicos, e apenas indiretamente o direito a segurança. E ainda quando possível a adequação de atos ciberterroristas a esses tipos penais, a toda evidência a sanção penal se afigura desproporcional, insuficiente enquanto prevenção e reprovação da conduta.

Neste cenário, a exclusão dos servidores e redes individuais do âmbito de proteção da Lei 13.260/16 configura uma vio-

lação à proibição de proteção deficiente. Se, por um lado, o Estado brasileiro, ao editar a citada legislação, atendeu ao mandado expresso de criminalização do terrorismo, enunciado no artigo 5º, XLIII, da Constituição Federal, por outro, o fez de maneira insuficiente e, pois, desproporcional, posto que manteve sem proteção uma parcela importante do bem jurídico exposto a risco por condutas dessa natureza.

Com efeito, compreendido que os atos ciberterroristas afetam o direito fundamental à segurança, na sua perspectiva social, de direito a prestações positivas do Estado que minimizem os riscos inerentes à paz pública e à incolumidade pública, então a exclusão dos servidores privados do âmbito de proteção gera a inafastável consequência de que a disseminação de terror por intermédio de *spywares* introjetados em computadores de uso individual não configura ciberterrorismo. Poderá, a depender do caso, encontrar adequação típica aos artigos 154-A ou 266 do Código Penal. No primeiro cenário, se estará diante de infração penal de menor potencial ofensivo; no segundo, de crime de médio potencial ofensivo. Em ambos os cenários, evidentemente, a resposta penal será insuficiente à gravidade abstrata da conduta.

CONSIDERAÇÕES FINAIS

O desenvolvimento do presente estudo permite, sem a pretensão de esgotar a análise da matéria, responder ao problema inicial da pesquisa.

O ciberterrorismo assume importância e justifica a intervenção penal do Estado no âmbito da atual sociedade de risco globalizada, pautada nas tecnologias da informação e da comunicação. A estabilidade da sociedade contemporânea está diretamente atrelada ao normal funcionamento dos recursos tecnológicos que estabelecem a dinâmica da comunicação globalizada, uma dinâmica de rede. É nesse contexto que o uso das ferramentas tecnológicas de comunicação, como a internet, ao degenerar para finalidades reprováveis, como a disseminação do medo e do terror, afeta a paz social e a incolumidade pública, e em

última instância o direito fundamental à segurança, atraindo a intervenção legítima do Direito Penal. Aliás, a legitimidade da intervenção penal é pressuposta pelo legislador constituinte, que incluiu mandado expresso de criminalização na Constituição Federal.

O ponto de reflexão está relacionado com a proporcionalidade estrito sensu da intervenção penal, como delineada na Lei 13.260/16, tendo como parâmetro o direito fundamental à segurança. E nesse ponto, em especial, a suficiência da proteção penal, tendo em vista o recorte do seu âmbito de proteção. Se, de um lado, não se identifica intervenção excessiva na mencionada lei, de outro, a exclusão dos servidores privados de uso individual do âmbito de proteção das suas normas configura uma proteção deficiente, posto que deixa desprotegida importante parcela dos servidores que integram a rede informática que materializa a comunicação na sociedade contemporânea.

Ainda que possível a adequação de atos de ciberterrorismo a tipos penais existentes no ordenamento jurídico-penal, como os artigos 154-A e 266 do Código Penal, certo é que nem sempre haverá essa subsunção. Outrossim, mesmo nas hipóteses em que tal for possível, as sanções penais revelam-se inequivocamente insuficientes à prevenção e à reprovação das condutas, o que evidencia a insuficiência do atual ordenamento jurídico-penal à proteção de bens jurídicos expostos a risco pelo ciberterrorismo.

Assim, não obstante o legislador brasileiro tenha materializado um comando constitucional – mandado explícito de criminalização – o fez de maneira insuficiente, tendo em vista o risco inerente ao ciberterrorismo e a vulnerabilidade de bens jurídicos excluídos do âmbito de proteção da norma.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXY, Robert. *Constitucionalismo Discursivo*. 4.ed. Trad. Luís Afonso Heck. Porto Alegre: Livraria do Advogado, 2015.

ASSMANN, Hugo. A metamorfose do aprender na sociedade da informação. *Revista Ciência da Informação - Ci. Inf.*, Brasília, v. 29, n. 2, p. 7-15, maio/ago. 2000, p. 7. Disponível em: <http://www.scielo.br/pdf/ci/v29n2/a02v29n2>.

BALTAZAR JUNIOR, José Paulo. *Crime Organizado e Proibição de Insuficiência*. Livraria do Advogado: Porto Alegre, 2010.

BARATTA, Alessandro. Seguridad. In: *Criminología y sistema penal* (compilación in memoriam). Editorial BdeF: Buenos Aires, 2004, p. 199-220.

BAUMAN, Zygmunt. *Medo Líquido*. Tradução: Carlos Alberto Medeiros. 1. Ed. Rio de Janeiro: Editora Zahar, 2008.

BECK, Ulrich. *Sociedade de Risco: rumo a uma outra sociedade*. Tradução: Sebastião Nascimento. 2. Ed. São Paulo: Editora 34, 2011.

CAMBI, Eduardo Augusto Salomão; AMBROSIO, Felipe Augusto Rodrigues. Lei Antiterror brasileira (l. 13.260/16): ameaça à democracia e aos direitos fundamentais. *Revista Quaestio Iuris*. vol. 10, n°. 03, Rio de Janeiro, 2017. pp. 1370-1397, p. 1371. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/24805/25799>.

CANOTILHO, Joaquim José Gomes. *Direito Constitucional e Teoria da Constituição*. 3.ed. Coimbra: Almedina, 1998.

CAPOBIANCO, Lígia. A Revolução em Curso: Internet, Sociedade da Informação e Cibercultura. *Revista de Estudos em Comunicação*, nº 7 - Volume 2, 175-193, Maio de 2010, p. 175. Disponível em: <http://www.ec.ubi.pt/ec/07/vol2/EC07-2010-vol2.pdf>.

CARTILHA DE SEGURANÇA PARA INTERNET. *Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil* – Cet.br. Disponível em: <https://cartilha.cert.br/malware/>.

CASTELLS, Manuel. *A sociedade em rede*. Tradução: Roneide Venâncio Majer; atualização para a 6ª edição: Jussara Simões - (A era da informação: economia, sociedade e cultura; v.1) São Paulo: Ed. Paz e Terra, 1999.

COSTA, Alan Denilson Lima. Ciberterrorismo. In: VASCONCELOS, Carlos Eduardo de Oliveira (org.). *Terrorismo e outras situações de emergência*: Teoria e prática da prevenção e do combate. Escola Superior do Ministério Público da União – ESMPU, 2018, p. 171-172. Disponível em: http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Biblioteca_Virtual/Livros_Digitais/ESMPU%203422_EBOOK%2BTERRORISMO.pdf.

D'ÁVILA, Fábio Roberto. Liberdade e segurança em direito penal. O problema da expansão da intervenção penal. *Revista Eletrônica de Direito Penal*. Ano 1, vol. 1, nº 1, jun. 2013, p. 66. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/redpenal/article/view/7142/5118>.

DE GIORGI, Raffaele. The risk of risk society and the limits of law. In: *Direito Fundamental à Segurança e Direitos de Liberdade: a complexa harmonia em matéria penal* [recurso eletrônico]. MAYA, André Machado; LORENZONI, Pietro Cardia (Orgs). Págs. 39-50. Porto Alegre: FMP, 2019.

DENNING, Dorothy Elizabeth. *Cyberterrorism*. Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 Maio 2000, tradução nossa. Disponível em: <https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm>.

Dicionário Michaelis. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/terror>. Acesso em 08 abr. 2019.

FALCÃO JÚNIOR, Alfredo Carlos Gonzaga; BUFFON, Jaqueline Ana. *Ciberterrorismo: entre a prevenção e o combate*. In: SILVA, Ângelo Roberto Ilha da (org.). *Crimes cibernéticos*. 2.ed. Porto Alegre: Editora Livraria do Advogado, 2018.

FLOR, Roberto. Perspectiva para novos modelos de "investigação tecnológica" e proteção de direitos fundamentais na era da internet o chamado "ciberterrorismo" como um primordial exemplo, em conjunto a problemas de definição e a luta contra terrorismo e os crimes cibernéticos. *Revista dos Tribunais. Revista Brasileira de Ciências Criminais*: RBCCrim, v. 20, n. 99, p. 69-100, nov./dez. 2012.

GIDDENS, Anthony. *Modernidade e identidade*. Tradução: Plínio Dentzien. Rio de Janeiro: Editora Zahar, 2002, Base de Dados Minha Biblioteca.

GORDON, Sarah; FORD, Richard. *Cyberterrorism?*. *Computers & Security*, [S.l.] v. 21, Issue 7, p. 636-647, nov. 2002.

GOUVEIA, Luis Manoel Borges. *Sociedade da informação: Notas de contribuição para uma definição operacional*. Universidade Fernando Pessoa, Portugal, 2004, p. 1. Disponível em: http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf.

GUZELLA, Thatiana Laiz. *A expansão do direito penal e a sociedade de risco*. Publica Direito. Brasília, Distrito Federal, nov. 2008, p. 3073. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/brasil/13_357.pdf.

HARDY, Keiran; WILLIAMS, George. What is “Cyberterrorism”? Computer and Internet Technology in Legal Definitions of Terrorism. In: CHEN, Thomas e alt. *Cyberterrorism, Understanding, Assessment, and Response*. London: Springer, 2014.

HUNGRIA, Nélon. *Comentários ao Código Penal*. Vol. IX. Arts. 250 a 361. Revista Forense. Rio de Janeiro, 1959.

KALAC, Jasmin. Cyber-terrorism as a threat to national security. *International Refereed Scientific Journal Vision*, Volume 2, Issue 2, September 2017, p. 119-127, p. 120, tradução nossa. Disponível em: http://visionjournal.edu.mk/wp-content/uploads/2018/03/irsjv_v2i2_jasmin.pdf.

LEAL, Rogério Gesta. *A responsabilidade penal do patrimônio ilícito como ferramenta de enfretamento da criminalidade*. E-book. Fundação Escola Superior do Ministério Público, Porto Alegre, 2017, p. 41-42. Disponível em: https://www.fmp.edu.br/wp-content/uploads/2017/10/responsabilidadepenal_EBOOK.pdf.

LIMA, Renato Brasileiro de. *Legislação criminal especial comentada: volume único*. 6 Ed. ver., atual e ampl. Salvador: JusPODIVM, 2018.

MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth. *Cyberterrorismo: a nova era da criminalidade [Coleção Cybercrimes]* – 1 reimp. Belo Horizonte: Editora D’Plácido, 2018.

MAYA, André Machado. O processo penal na sociedade de risco: a persecução penal no Brasil entre os ideais de liberdade e segurança. *Revista de Estudos Criminais*, ano 2019, v. 18, nº 73, p. 179-219.

MAYA, André Machado; LORENZONI, Pietro Cardia. Direito (fundamental) à segurança? Uma aproximação a partir da jurisprudência do Tribunal Constitucional brasileiro e da Corte Interamericana de Direitos Humanos. In: *O direito penal e o processo penal como instrumentos de defesa de direitos públicos incondicionados: perspectivas brasileiras e chilenas* [recurso eletrônico]. LEAL, Rogério Gesta, sbardelotto, Fábio Roque; ÁLVARES, Rodrigo Ríos (Orgs.). Págs. 239-266. Porto Alegre: FMP, 2019.

PONTE, Antonio Carlos da; KAZMIERCZAK, Luiz Fernando. Terrorismo: análise da lei nº 13.260/16. *Revista Jurídica ESMP-SP*, São Paulo, v.11, 2017: 132 – 148, p. 145. Disponível em: http://www.esmp.sp.gov.br/revista_esmp/index.php/RJESMPSP/article/download/345/172.

SILVA SÁNCHEZ, Jesús Maria. *A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais*. Tradução: Luiz Otávio de Oliveira Rocha. – São Paulo: Editora Revista dos Tribunais, 2002.(Série as ciências criminais no século XXI, v.11).

SOUZA NETO, Cáudio Pereira de. Comentários ao artigo 5º da Constituição Federal brasileira. In: CANOTILHO, J.J. Gomes; SARLET, Ingo Wolfgang, STRECK, Lenio Luiz, MENDES, Gilmar Ferreira (Orgs). *Comentários à Constituição Federal brasileira*. São Paulo: Saraiva/Almedina, 2013.

TAKASHI, Tadao (Org.). *Sociedade da Informação no Brasil*: Livro Verde. Ministério da Ciência e Tecnologia, Brasília, 2000, p. 11. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/livroverde.pdf>.

TALIHÄRM, Anna-Maria. Cyberterrorism: in Theory or in Practice? *In: Defense Against Terrorism Review*. Vol.3, N° 2, Fall 2010, p. 59-74, p. 69, tradução nossa. Disponível em: http://www.coedat.nato.int/publication/datr/volume6/05-Cyberterrorism_in_Theory_or_in_Practice.pdf.

VEIGA, Eduardo de Lima. *Terrorismo e direito penal do inimigo: contornos e legitimidade à luz do direito internacional*. Dissertação (Mestrado em Direito)– Programa de Pós-Graduação em Direito, Fundação Escola Superior Do Ministério Público, Porto Alegre, 2018.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Revista Ciência da Informação - Ci. Inf.*, Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000, p. 71. Disponível em: <http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf>.