CIBERCRIMES E CIBERTERRORISMO: A POTENCIAL ATUAÇÃO LEGISLATIVA NO ORDENAMENTO JURÍDICO BRASILEIRO

PERIOLO, João Felipe[1]
REZENDE, Guilherme Carneiro de[2]

RESUMO

O presente trabalho tem como objetivo apresentar e discutir hipóteses possíveis de atuação estatal no combate ao cibercrime e ao ciberterrorismo, entre outras ameaças praticadas por meio das tecnologias de informação e comunicação virtuais. No cenário internacional de enfrentamento ao terrorismo, outros países sofreram ataques perpetrados por intermédio, ou com auxílio, da tecnologia de comunicação conectada à rede mundial de computadores e, por esse motivo, desenvolveram métodos para coibirem a atuação de agentes criminosos que conseguiram causar uma situação de terror na população. Em contrapartida, o Estado Brasileiro possui escassos exemplos de legislações voltadas à proteção da sociedade em ambiente virtual, tendo recentemente promulgado a Lei Geral de Proteção de Dados Pessoais - LGPD, essa que somente dispõe sobre sanções administrativas para infrações no uso de dados pessoais em ambiente virtual. Não obstante, a LGPD inovou no ordenamento jurídico nacional, ao criar a Autoridade Nacional da Proteção de Dados – ANPD, órgão estatal com capacidade de ser, futuramente, convertida numa autarquia especial, que tem um potencial decisivo para a atuação do poder executivo no enfrentamento a possíveis crimes em ambiente virtual, já que muitos deles utilizam a exposição e vulnerabilidade dos dados pessoais armazenados nesse meio para se consumarem.

PALAVRAS-CHAVE: cibercrime, ciberterrorismo, segurança de dados.

1 INTRODUÇÃO

A proteção dos brasileiros contra crimes e atos terroristas cometidos por intermédio, ou com auxílio, da internet encontra-se defasada com omissão e obscuridade nas legislações nacionais pertinentes e, em especial, na própria definição das práticas de crimes consideradas terroristas que não se apresentam de forma consensual no ordenamento jurídico do país.

Para o FBI – *Federal Bureau of Investigation*, entende-se como terrorismo a prática ou ameaça de atos criminosos, cometidos por grupos ou indivíduos, associados a organizações internacionais ou domésticas, que o fazem com o objetivo de causar terror à população, motivados por questões ideológicas, entre elas, de natureza política, religiosa, social, racial ou ambiental.

Já o ciberterrorismo, conforme definição também do FBI, seria qualquer ataque politicamente motivado e executado de forma premeditada "contra informação, sistemas de computadores, programas computacionais e bancos de dados que resultem em violência contra alvos não-combatentes por grupos subnacionais ou agentes clandestinos" (COE-DAT, 2008, pg.119, tradução nossa).

[1]Acadêmico do Curso de Direito – **Centro Universitário Assis Gurgacz** – Cascavel/PR – jfperiolo@minha.fag.edu.br.com
[2]Professor Mestre do Curso de Direito – **Centro Universitário Assis Gurgacz** – Cascavel/PR – guilhermerezende@fag.edu.br

Vítima de inúmeros ciberataques perpetrados por agentes externos nas últimas duas décadas, conforme relatado pela CSIS - *Center for Strategic & International Studies*, os Estados Unidos da América criaram, no ano de 2018, a CISA – *Cybersecurity and Infrastructure Security Agency*, agência subordinada ao governo federal daquele país, responsável por coordenar e fortalecer ações de proteção a ataques cibernéticos.

Considerando as definições norte-americanas para as práticas de terrorismo e ciberterrorismo, além da criação da CISA, exemplo de atuação estatal para a proteção de dados e o combate a esses crimes em território nacional, entende-se como necessário discutir as opções que o Estado Brasileiro tem para, preventivamente, criar mecanismos legais capazes de fazerem o mesmo.

Da mesma forma, é importante considerar que, tratando-se de situações criminosas, elas, obrigatoriamente, devem ser penalizadas por leis no sentido estrito, advindas de forma exclusiva do poder legislativo federal, conforme o princípio da legalidade exposto no art. 5º, inciso XXXIX, da Carta Magna.

O presente trabalho também expõe exemplos de ataques executados contra órgãos do governo brasileiro, supostamente perpetrados tanto por agentes nacionais como estrangeiros, além de ataques sofridos contra o governo de outros países, em especial, dos localizados no leste europeu, nos quais os métodos utilizados para o combate a esses crimes serviram de exemplo para o estudo de práticas efetivas de prevenção contra futuros ataques cibernéticos.

Com os exemplos apresentados, será possível propor hipóteses que terão a capacidade de prevenir ataques contra o Estado Brasileiro, por meio de novos marcos legislativos, bem como avançar demais discussões sobre o tema em ambiente jurídico e acadêmico.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 DEFINIÇÕES INTERNACIONAIS PARA O CIBERCRIME E O CIBERTERRORISMO

É possível extrair diversos conceitos estabelecidos por atores no âmbito do direito internacional, entre eles a ONU - Organização das Nações Unidas, que tipificam o cibercrime e ciberterrorismo praticados com efeitos e conexões internacionais. Em particular, o UNODC - Escritório das Nações Unidas sobre Drogas e Crimes- define o cibercrime como ato ilícito cometido por meio da ICT - Informação e Comunicação Tecnológica- propagado na Rede

Mundial de Computadores, ou WWW - *World Wide Web*, em inglês, bem como, pode ser uma ferramenta para facilitar o cometimento de atos terroristas.

> Particularmente, a Internet pode ser usada para fins terroristas, como a disseminação de "propaganda (incluindo recrutamento, radicalização e incitação ao terrorismo); financiamento [terrorista]; treinamento [terrorista]; planejamento [de ataques terroristas] (inclusive por meio de comunicação secreta e informações de código aberto); execução [de ataques terroristas]; e ataques cibernéticos" (UNODC, 2019, tradução nossa)

De modo similar, retomando o conceito do FBI disposto na introdução, o ciberterrorismo pode ser definido como o crime que ataca os meios de comunicação e informações virtuais, disseminados e acessíveis em nível mundial em que indivíduos e entidades, nacionais ou estrangeiros, cometem com o específico objetivo de causar “estado de terror no público em geral, em um grupo de pessoas ou em determinadas pessoas para fins políticos” (AGNU, 1960).

Diante do exposto, também é possível fazer uma analogia entre a definição da prática de terrorismo, extraída da resolução 49/1960 da AGNU - Assembleia Geral das Nações Unidas, com as definições da UNODC e FBI supracitadas, em que o ciberterrorismo seria o ato criminoso que utiliza a ICT para divulgação de propaganda, financiamento, radicalização e incitação entre outros atos terroristas praticados em meios tanto virtuais quanto reais.

2.2 EXEMPLOS LEGISLATIVOS NACIONAIS DE COMBATE AOS CIBERCRIMES E CIBERTERRORISMO

No Brasil, é possível encontrar a definição para prática de terrorismo na Lei n° 13.260/2016, em seu artigo 2°, a qual, embora limita sua tipificação apenas quando o ato for cometido por “razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião”, tipifica as condutas que são consideradas como atos terroristas em seu § 1º, entre elas, os atos praticados por meio de “mecanismos cibernéticos”, em seu inciso IV.

> IV - sabotar o funcionamento ou apoderar-se, com violência, grave ameaça à pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento. (Art. 2°, §1, inciso IV, da Lei 13.260/16)

A lei também comina penas a esses crimes tipificados no § 1º do art. 2° e define que esses crimes são de competência da União. Desse modo, a Polícia e a Justiça Federal são responsáveis por investigar e julgar, respectivamente, os crimes previstos nessa lei.

Os artigos 16 e 17 também definem que o processamento das ações penais deverá ser feito conforme a Lei n° 12.850/2013, que rege sobre o combate às organizações criminosas, e a Lei 8.072/1990 dos crimes hediondos, equiparando os atos terroristas a essas modalidades penais já inseridas previamente no ordenamento jurídico nacional.

Da mesma forma, outra lei que apresenta omissão em relação à responsabilidade penal no cenário virtual é a Lei Geral de Proteção de Dados Pessoais – LGPD, Lei n° 13.709/2018, que dispõe sobre normas para o tratamento de dados pessoais armazenados ou processados de forma virtual, nos limites do território brasileiro.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Art. 1°, caput, da Lei 13.709/18)

Embora garanta uma segurança jurídica contra a exploração comercial de dados sensíveis da população geral, que cada vez mais se encontra submetida a serviços que necessitam de acesso a informações virtuais, a LGPD ainda não dispõe sobre sanções penais contra ações criminosas que os fornecedores desses serviços ou terceiros, possam cometer atuando nessas situações, limitando-se apenas a sanções administrativas.

No entanto, destaca-se a importância da criação da Autoridade Nacional de Proteção de Dados – ANPD, órgão subordinado ao poder executivo, criado pela LGPD. Sua função de "zelar pela proteção de dados" e "fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação", contidas nos incisos I e IV, do art. 55-J, respectivamente, que demonstra o interesse inaugural do Estado em promover a segurança de dados pessoais em meio virtual, além de salvaguardar uma possível expansão da atuação da ANPD para esse fim, especificado no § 1º, do art. 55-J, possibilitando sua conversão em uma autarquia especial subordinada à Presidência da República.

É também possível mencionar a Lei n° 14.155, de 27 de maio de 2021, que proporcionou alterações no Código Penal Brasileiro (CP), tipificando novos ilícitos, bem

como agravando as penas cominadas aos crimes de violação de dispositivo informático, conectados ou não à rede, como furto e estelionato cometidos em ambiente eletrônico ou virtual.

> Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações: "Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. [...] (Art. 1°, da Lei n° 14.155/21)

Outrossim, essa lei criou o tipo penal de "fraude eletrônica", que além de resultar na aplicação da pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, também possui majorante que considera a magnitude do resultado gravoso, caso o crime seja "praticado mediante a utilização de servidor mantido fora do território nacional", conforme nova redação do § 2º-B, do art. 171, do CP.

2.3 ANÁLISE DO CRIME DE TERRORISMO PELO AUTOR FERNANDO CAPEZ

O Dr. Fernando Capez, em seu livro sobre Legislação Penal Especial, 16° edição, do ano de 2021, discorre sobre a relevância em delimitar os atos terroristas com base em definições tanto nacionais quanto internacionais, bem como também menciona que a internet tem o potencial de ser uma ferramenta aliada aos criminosos para o planejamento desses atos.

No cenário internacional, o autor destaca os efeitos do terrorismo, que "não se limitam mais ao Estado em que foi cometido", e, assim, na tentativa de estabelecer uma definição para ele, diversos atores internacionais, por meio da Convenção de Genebra de 1937 e Resolução n° 1.373 do Conselho de Segurança da ONU, tentaram categorizar os atos terroristas como crimes contra a humanidade, necessitando da criação de uma jurisdição especial, com instrumentos jurídicos eficazes para julgá-los e preveni-los.

Já no Brasil, Capez menciona os marcos legislativos adotados no ordenamento jurídico nacional para combater o terrorismo, e, em especial, realiza a análise da Lei n° 13.260/2016, mencionada em capítulo anterior do presente artigo.

Em relação à objetividade jurídica, o autor trouxe em discussão a possibilidade do enquadramento em natureza política dos atos terroristas, embora necessite da conjunta interpretação análoga à Lei 7.170/83 - Lei dos Crimes contra a Segurança Nacional, que rege,

como necessário, para se caracterizarem como crimes políticos, as hipóteses de lesão real ou potencial “à integridade territorial e soberania nacional”; “ao regime representativo e democrático, à Federação e ao Estado de Direito” e “às pessoas dos chefes dos Poderes da União”.

Do ponto de vista processual penal, conforme relembrado por Capez, aos atos terroristas aplicam-se também os dispositivos da Lei 8.072/1990 - Lei dos Crimes Hediondos, em razão do tratamento severo exigido pelo art. 5°, XLII, da CF/88, bem como os da Lei 12.850/2013 - Lei das Organizações Criminosas, quando se tratar do processo contra organizações terroristas.

Ademais, é mencionado pelo autor o Projeto de Lei do Senado Federal, n° 272 de 2016, que pretende ampliar o rol de condutas consideradas como terroristas, para além do já disposto pela Lei n° 13.260/2016, em “incendiar, depredar, saquear, destruir ou explodir meios de transporte ou qualquer bem público ou privado, e os atos de interferir, sabotar ou danificar sistemas de informática ou bancos de dados (CAPEZ).

2.4 DISCUSSÃO SOBRE SEGURANÇA INFORMÁTICA PELO AUTOR ANDRÉ ESTEFAM

O promotor de justiça e Dr. André Estefam elaborou discussões a respeito do crime de Invasão de Dispositivo Informático, cominado no Art. 154-A, do Código Penal, em seu livro Direito Penal 2 - Parte Especial. Trata-se de um crime que, segundo o autor, criou um novo bem jurídico penal, a segurança informática, e, após a publicação da Lei n° 12.737/2012 que o instituiu, o artigo sofreu novas alterações no ano de 2021, que agravaram as penas cominadas às práticas estipuladas em seu texto.

Estefam menciona a revolução digital como sendo a responsável pelo “surgimento de uma nova forma de criminalidade: os delitos informáticos”. Importante destacar o raciocínio do autor, de que o direito se amolda à realidade, e que aos poucos é modificado para proteger novos bens jurídicos, bem como, com a introdução da sociedade aos novos meios digitais, diversos ramos do direito já evoluíram para acompanhar essas mudanças sociais.

Da mesma forma que no Direito Civil, no Direito Comercial e no Direito do Consumidor foram criados novos dispositivos legais para atender à necessidade da sociedade digital; no Direito Penal houve a necessidade de acompanhá-la criando tipificações para punir os delitos praticados por meios informáticos.

O autor também menciona que, por algum tempo, foram possíveis enquadrar práticas criminais realizadas por meios informáticos em tipos penais já existentes que protegiam bens jurídicos já conhecidos pelo direito como a privacidade, o patrimônio, a propriedade material, entre outros, sem ainda necessitarem ser estipulados novos bens. No entanto, com a falta de tipificações para esses crimes, o autor explica que alguns ilícitos praticados nesses meios caracterizavam condutas atípicas, que não poderiam ser punidas pelo direito penal:

> Havia, porém, uma considerável gama de comportamentos ilícitos praticados no ambiente informatizado que se mostravam atípicos e, em virtude da proibição de analogia in malam partem, não poderiam ser açambarcados pelo manto protetivo do Direito Penal, senão por meio de uma reforma legislativa. (ESTEFAM, 2022)

Dessa forma, a solução dos legisladores foi a tipificação de novas condutas ilícitas que, como no caso da Lei n° 12.737/2012, estabeleceu o bem jurídico da Segurança Informática, esse que é conjuntamente relacionado à proteção de outros bens, como o da privacidade, da intimidade, da autodeterminação informática, que, segundo o autor, seria "a liberdade de transitar no ambiente virtual a salvo da intervenção indevida de terceiros".

Importante salientar o objeto material que a supracitada lei protege, o dispositivo informático, que, conforme explicitado por Estefam, seria o "mecanismo físico ou virtual capaz de reunir informações ou dados digitalizados em ambiente eletrônico por meio da linguagem característica dos computadores e mecanismos equivalentes". Dessa forma, necessariamente por meio ou com auxílio desses dispositivos, conectados ou não em redes privadas ou de internet, tais ilícitos mencionados nessa lei, bem como outros crimes virtuais e atos terroristas expostos no presente artigo, necessariamente se consumariam.

2.5 EXEMPLOS INTERNACIONAIS DE COMBATE AO CIBERCRIME

Na tentativa de enfrentar ataques cibernéticos contra nações aliadas, a OTAN criou a CCDCOE - *Cooperative Cyber Defence Centre of Excellence,* ou Centro de Excelência De Ciberdefesa Cooperativa, na tradução em português, com sede na cidade de Tallinn, capital da Estônia.

Em especial, esse país, que sedia a CCDCOE, entrou na OTAN no ano de 2007 e possui um histórico de ataques cibernéticos sofridos no mesmo ano que foram capazes de

derrubar a internet em seu território, assim como nos outros dois países da região dos bálticos, Lituânia e Letônia (MARSILI, 2018).

Com a experiência obtida no enfrentamento aos ciberataques, a CCDCOE publicou, no ano de 2013, o Manual de Tallinn, obra que possui o histórico dos ataques sofridos pelo país da Estônia, assim como apresenta um estudo compilado de como as legislações internacionais podem ser aplicadas nesses casos. Essa mesma obra encontra-se frequentemente sendo atualizada, com uma segunda publicação feita no ano de 2017, e uma terceira que ainda está sendo desenvolvida (CCDCOE).

O major do exército americano, Willian C. Ashmore, no artigo intitulado "*Impact of Alleged Russian Cyber Attacks"* – Impacto dos Alegados Ciberataques Russos, na tradução do título em português, comenta que o ataque do ano de 2007 contra a Estônia seria "a primeira ciberguerra da história", detalhando que os ataques seriam perpetrados pelo Kremlin, sede do governo russo, ou por indivíduos ligados a ele, em retaliação à decisão do governo estoniano de retirar um monumento soviético do centro de sua capital.

Ashmore também expôs em seu artigo os ataques subsequentes a outros três países democráticos no leste da Europa e na Ásia central: Geórgia, Lituânia e Quirguistão, entre os anos de 2008 e 2009, países pertencentes à, já extinta, União Soviética até 1991, que, segundo o mesmo autor, teriam sido perpetrados por indivíduos ligados ao governo russo.

> A existência de hackers que apoiam o governo russo e especialistas em informação dentro do governo russo criaram um ativo que será usado durante futuros conflitos cibernéticos. A ênfase do governo russo no desenvolvimento de estratégias cibernéticas permitirá que a Rússia esteja preparada para futuros conflitos cibernéticos. (Ashmore, 2009, tradução nossa)

A Organização das Nações Unidas, de forma reiterada, também demonstrou preocupação sobre a necessidade de se combater o cibercrime por meio da *Comission on Crime Prevention and Criminal Justice* (CCPCJ), ou Comissão de Prevenção de Crime e Justiça Criminal em português, assim como já organizou a Convenção Internacional sobre o Cibercrime, em 2010.

No décimo terceiro Congresso sobre a Prevenção de Crimes e Justiça Criminal, realizado no ano de 2015, os países membros da ONU discutiram sobre o mesmo tema, sendo que nessa oportunidade, o cibercrime e o ciberterrorismo foram expostos de maneira conjunta na intenção de caracterizar esse último como sendo uma forma autônoma de ato terrorista,

ainda que nele se obtenha o resultado “terror”, sem que, necessariamente, seja executado de forma violenta (MARSILI, 2018).

2.6 ATAQUES CIBERNÉTICOS RECENTES CONTRA ÓRGÃOS DO GOVERNO

Diferentes órgãos do governo brasileiro sofreram ataques cibernéticos nos últimos anos, em decorrência do uso cada vez maior de meios digitais para o armazenamento de dados. Entre os exemplos mais notórios, o Superior Tribunal de Justiça – STJ, o Tribunal Superior Eleitoral – TSE, e diferentes Tribunais Regionais do Trabalho – TRTs tiveram seus bancos de dados sequestrados por agentes estrangeiros e nacionais, conforme listados a seguir, noticiados por meio do canal de notícias do STJ, do site da revista VEJA e do G1.

Em novembro de 2020, os servidores responsáveis pelos processos digitais e armazenamento de dados do STJ foram vítimas de um *ransomware* – “programa malicioso criado para sequestrar dados em dispositivos” (AVAST), causando diversos transtornos para a corte, incluindo o adiamento de sessões por videoconferência das seis turmas julgadoras, além da suspensão de prazos processuais, obrigando a corte funcionar em regime de plantão presencial (STJ).

Da mesma forma, em junho de 2020, o site do TSE foi vítima de um ataque cibernético conhecido como *defacement* – “ataque em que indivíduos penetram no domínio do website e mudam o conteúdo, introduzindo as próprias mensagens, na tentativa de propagar suas ideologias ou causar transtornos para os donos do site” (IMPERVA), sendo que nessa situação, os autores do crime, prontamente identificados como brasileiros, foram detidos pela Polícia Federal – PF no mês de agosto do mesmo ano (VEJA).

Também é pertinente trazer à mostra alguns dos diversos ataques cibernéticos sofridos por diferentes tribunais regionais, tanto Tribunais Regionais do Trabalho – TRTs ou Tribunais Regionais Federais, TRFs. Como exemplo, é possível mencionar o ataque recente ao Tribunal Regional Federal da 3ª Região, do estado de São Paulo, que, na data de 30 de março de 2022, teve seus servidores digitais invadidos e colocados fora do ar por indivíduos até então desconhecidos. Conforme noticiado pelo site do G1, a Polícia Federal esteve no prédio do TRF-3, ainda no mesmo dia do ataque, para investigar a extensão dos danos e, posteriormente, instaurar um inquérito policial.

De acordo com matérias noticiadas pelo G1, os Tribunais Regionais do Trabalho do estado do Rio Grande do Sul e do Espírito Santo, TRT-RS e TRT-ES, respectivamente, também foram vítimas de crimes executados de forma muito semelhante. Da mesma forma,

nessas ocasiões, foram realizadas práticas de isolamento desses servidores, os quais continham diversos dados pessoais e processuais das ações em andamento, mostrando-se eficazes para evitar que sua integridade ou sigilo fossem comprometidos.

Muito embora nesses crimes praticados contra o TRF-3, TRT-RS e TRT-ES foram tomadas medidas de isolamento de dados, assim como investigações foram iniciadas pela Polícia Federal, conforme relatado pelas matérias jornalísticas supracitadas, os ataques cibernéticos impossibilitaram o trabalho presencial e ininterrupto de desembargadores e outros funcionários desses órgãos do judiciário, obrigando-os a suspenderem os prazos processuais por algum tempo, gerando enorme transtorno aos dependentes da justiça.

2.7 HISTERIA MIDIÁTICA BRASILEIRA SOBRE POSSÍVEIS FUTUROS E INCERTOS ATAQUES CIBERTERRORISTAS

Há poucos meses, antes das Eleições Gerais do Brasil de 2022, o Ministro Edson Fachin, do STF, tomou posse como presidente do TSE – Tribunal Superior Eleitoral e em entrevista ao jornal Estadão, acessada pelo site da ISTOÉ - Dinheiro, o ministro expôs a ameaça de possíveis ataques cibernéticos iminentes contra o TSE, considerando o histórico de diferentes ataques sofridos pelos outros órgãos do judiciário.

No entanto, sem demonstrar provas concretas, o ministro fez acusações contra o país da Rússia, além de outros agentes estatais estrangeiros, como sendo propícios a incentivarem esses possíveis ataques.

> A preocupação com o ciberespaço se avolumou imensamente nos últimos meses e eu posso dizer a vocês que a Justiça Eleitoral já pode estar sob ataque de hackers, não apenas de atividades de criminosos, **mas também de países, tal como a Rússia, que não tem legislação adequada de controle.** (Min. Edson Fachin, em entrevista ao Estadão, grifo nosso)

A fala do ministro reflete seu ponto de vista político ante as eleições gerais de 2022, que, por meio de entrevistas, ainda que sejam compartilhadas pela internet, contam com a autoridade da velha imprensa tradicional, muito embora também seja real a necessidade de se garantir a máxima segurança e lisura no processo eleitoral, que cada vez mais depende de tecnologias de informática, suscetíveis a ataques cibernéticos.

Conforme apresentado por uma matéria jornalística da revista Veja, realizada no mês de março de 2022, poucos dias após o Min. Fachin assumir a presidência do TSE,

supostamente, os técnicos do tribunal já teriam informações de que seus servidores seriam alvos prioritários, estando na iminência de serem vítimas de "terrorismo digital", durante os dias de votação. Novamente, essa matéria jornalística é mais uma que apresenta comentários politizados, bem como em entrevista o Min. Fachin, injustificadamente, voltou a acusar outras nações estrangeiras de serem responsáveis por ataques, que sequer aconteceram, em comentários como "Há riscos de ataques cibernéticos ao TSE de diversas origens, inclusive favorecidos por nações" e "A Rússia é um exemplo dessas procedências e tem resultado em sancionar os cibercriminosos".

Em particular, esse último comentário apresentado pelo ministro acaba por ser rebatido com as informações atribuídas à atuação do Serviço Federal de Segurança da Federação Russa – FSB no enfrentamento a verdadeiros ciberterroristas, que culminou na prisão de membros do grupo hacker *REvil*, em janeiro de 2022, conforme divulgado pelos canais de notícia europeus *Deutsche Welle* – DW e *Russia Today* – RT.

De acordo com a DW e RT, os membros do grupo *REvil* foram responsáveis pelo sequestro de contas bancárias da empresa multinacional de origem brasileira, a JBS S.A., no ano de 2021, bem como alguns de seus membros, conforme relatado por oficiais do próprio governo americano, estariam também envolvidos no ataque que causou a interrupção do fornecimento do maior sistema de distribuição de gás natural dos Estados Unidos, a *Colonial Pipeline*, naquele mesmo ano.

Ainda, conforme noticiado pela DW, nessa operação da FSB, foram cumpridos 25 mandados de busca e apreensão, sendo apreendidos 14 indivíduos e mais de 426 milhões de rublos, valor aproximado de 5.6 milhões de dólares na época dos fatos. A atuação do serviço de segurança russo teria sido uma cooperação com o próprio governo americano, após o encontro dos respectivos presidentes Vladimir e Joe Biden, na cidade suíça de Genebra, também em 2021.

Diante desses exemplos de contraste, entre acusações infundadas e informações providas por canais de notícias nacionais e estrangeiros, torna-se possível expor uma fração da incoerência na troca de informações no sistema de comunicação digital, que acaba por ser uma das fragilidades para aqueles que dependem delas. Frente a informações ambíguas encontradas em matérias jornalísticas enviesadas, disponibilizadas no meio digital, torna-se difícil para o público distingui-las entre si ou confirmarem as informações "[...]da rede com a realidade que está ao seu alcance" (MASAMUNE, 1995).

3 CONSIDERAÇÕES FINAIS

Como mencionado em sede do resumo deste artigo, o objetivo principal do trabalho é demonstrar a importância em se garantir a segurança jurídica frente a crimes e atos terroristas perpetrados por meio da ICT – Informação e Comunicação Tecnológica, por meio de legislações nacionais que tratem sobre o direito penal material e processual.

No presente artigo foram apresentadas algumas definições e exemplos de ataques cibercriminosos sofridos por entidades estrangeiras e internacionais, esses que enfrentaram os problemas e ameaças advindos de crimes cibernéticos supostamente perpetrados por atores inimigos de suas políticas externas, como citados os exemplos da Estônia e outros países bálticos com outros membros da OTAN, que foram obrigados a criar o CCDCOE, um centro responsável por coordenar extensivos estudos, na tentativa de coibir novos ataques.

Da mesma forma, foram compilados exemplos recentes de ataques cibernéticos sofridos por órgãos do governo brasileiro que exemplificam a necessidade de se promoverem soluções tanto administrativas, referentes a cada órgão, quanto legislativas, relacionadas a possíveis responsabilizações civis e penais, no intuito de prevenir, amenizar ou corrigir os resultados dos atos criminosos praticados. É importante ressaltar que os crimes que lesionam de forma direta o Estado, lesionam de forma indireta a coletividade que depende do funcionamento efetivo dos serviços prestados pelo governo.

Não bastando os diversos exemplos de definições doutrinárias, legislações e ataques cibernéticos, tanto nacionais quanto internacionais, apresentados neste artigo, é necessário continuar com a promoção de pesquisas e debates acadêmicos a respeito do tema, para que, contando com a participação conjunta da sociedade e do Estado, seja possível garantir a segurança nos meios informáticos, sem a qual não será possível efetivar os direitos inerentes ao ser humano, frente à nova realidade digital.

REFERÊNCIAS

AVAST. Guia essencial sobre ransomware. **O que é ransomware?** Disponível em: https://www.avast.com/pt-br/c-what-is-ransomware. Acesso em 09 abr. 2022

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 10 nov. 2021.

BRASIL. **Lei n° 8.072, de 25 de julho de 1990**. Dispõe sobre os crimes hediondos, nos termos do art. 5°, inciso XLIII, da Constituição Federal, e determina outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8072.htm. Acesso em: 10 nov. 2021.

BRASIL. **Lei n° 13.260, de 16 de março de 2016**. Regulamenta o disposto no inciso XLIII do art. 5° da Constituição Federal, disciplinando o terrorismo [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 10 nov. 2021.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13260.htm. Acesso em: 10 nov. 2021.

BRASIL. **Lei n° 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Lei/L14155.htm. Acesso em: 12 nov. 2021.

CAPEZ, F. **Legislação penal especial**. 16. ed. São Paulo: Saraiva, 2021. E-book.

CISA - Cybersecurity and Infrastructure Security Agency. **Combating Cyber Crime**. Disponível em: https://www.cisa.gov/combating-cyber-crime. Acesso em: 08 nov. 2021

CISA - Cybersecurity and Infrastructure Security Agency. **Cybersecurity**. Disponível em: https://www.cisa.gov/cybersecurity. Acesso em: 08 nov. 2021.

COE-DAT - Centre of Excellence Defence Against Terrorism. **Responses to Cyber Terrorism**. NATO Science for Peace and Security Series. E: Human and Societal Dynamics. Amsterdã, Holanda. IOS Press, 2008. v. 34. p. 119. Disponível em: https://books.google.com.br/books?id=tFmxVnDhBRQC&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. Acesso em: 7 nov. 2021.

CSIS - Center for Strategic & International Studies. **Significant Cyber Incidents**. Disponível em: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Acesso em: 7 nov. 2021.

DW - Deutsche Welle. **US 'welcomes' Russian arrests of REvil ransomware gang**. Disponível em: https://www.dw.com/en/us-welcomes-russian-arrests-of-revil-ransomware-gang/a-60432637. Acesso em: 10 abr. 2022.

ESTEFAM, A. **Direito Penal 2 - Parte Especial**. 9. ed. São Paulo: Saraiva, 2022. E-book.

FBI - Federal Bureau of Investigation. **Terrorism**. Disponível em: https://www.fbi.gov/investigate/terrorism. Acesso em: 7 nov. 2021.

G1 - **Tribunal Regional do Trabalho do ES sofre ataque cibernético**. Disponível em: https://g1.globo.com/es/espirito-santo/noticia/2022/02/21/tribunal-regional-do-trabalho-do-es-sofre-ataque-cibernetico.ghtml. Acesso em: 09 abr. 2022

G1 - **TJ-RS diz que sistema de informática do tribunal foi alvo de ataque cibernético: 'É muito grave'**. Disponível em: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/29/tj-rs-diz-que-sistema-de-informatica-do-tribunal-foi-alvo-de-ataque-hacker-e-muito-grave.ghtml. Acesso em: 09 abr. 2022

G1 - **Tribunal Federal da 3ª Região, em SP, mantém trabalhos suspensos entre 4 e 12 de abril por causa de ataque hacker.** Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/04/01/tribunal-federal-da-3a-regiao-em-sp-mantem-trabalhos-suspensos-entre-4-e-12-de-abril-por-causa-de-ataque-hacker.ghtml. Acesso em: 09 abr. 2022

IMPERVA. Website Defacement Attack. **What is a Website Defacement**. Disponível em: https://www.imperva.com/learn/application-security/website-defacement-attack/. Acesso em: 09 abr. 2022.

ISTOÉ Dinheiro - **'A Justiça Eleitoral já pode estar sob ataque de hackers', diz Edson Fachin.** Disponível em: https://www.istoedinheiro.com.br/a-justica-eleitoral-ja-pode-estar-sob-ataque-de-hackers-diz-edson-fachin/. Acesso em: 09 abr. 2022

RT - Russia Today. **US responds to Russian arrest of ransomware hackers** Disponível em: https://www.rt.com/news/546113-usa-russia-hackers-arrested/. Acesso em: 09 abr. 2022.

STJ - Superior Tribunal de Justiça - **Em razão de ataque cibernético, STJ funcionará em regime de plantão até o dia 9**. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ata

que-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx. Acesso em: 09 abr. 2022

STJ - Superior Tribunal de Justiça - **STJ Notícias destaca reforço na segurança de informações digitais do tribunal após o ataque hacker.** Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04122020-STJ-Noticias-destaca-reforco-na-seguranca-de-informacoes-digitais-do-tribunal-apos-o-ataque%E2%80%AFhacker.aspx. Acesso em: 09 abr. 2022

MASAMUNE S. ***Ghost in the Shell 1.5 - Human Error Processer***. São Paulo, Editora JBC, 2019. p. 180.

UNODC - United Nations Office on Drugs and Crimes. Module 4: Criminal Justice Responses to Terrorism. Key Issues. Defining Terrorism. **Counter-Terrorism**. Education For Justice University Module Series. Disponível em: https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html. Acesso em: 3 nov. 2021.

UNODC - United Nations Office on Drugs and Crimes. Module 14: Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace. Key Issues. Cyberterrorism. **Cybercrime**. Education For Justice University Module Series. Disponível em: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html. Acesso em: 3 nov. 2021.

VEJA - **A ameaça é real: TSE aciona o alerta contra a ação de terroristas digitais**. Disponível em: https://veja.abril.com.br/politica/a-ameaca-e-real-tse-aciona-o-alerta-contra-a-acao-de-terroristas-digitais/. Acesso em: 10 abr. 2022.