EM TEMPO
INSS – 1984 – 7858 DIGITAL
v. 21 n. 01

CRIMINALIDADE DIGITAL NO BRASIL: A PROBLEMÁTICA E A APLICABILIDADE DA CONVENÇÃO DE BUDAPESTE.

DIGITAL CRIMINALITY IN BRAZIL: THE PROBLEM AND APPLICABILITY OF THE BUDAPEST CONVENTION

Rafael Khalil Coltro[1]

Ricardo Libel Waldman[2]

RESUMO
O presente artigo aborda questões relativas à crescente criminalidade virtual no Brasil e no mundo, demonstrando que as condutas lesivas praticadas pelas redes virtuais se mostram cada vez mais perceptíveis mundos a fora. Assim, sabendo que o ambiente virtual se trata de uma rede mundialmente interligada, e do especial papel a ser desempenhado pelos estados em face dos novos desafios inerentes à essa nova época digital, muitos estados perceberam, de maneira precisa, que a única forma de exercer uma tutela jurisdicional efetiva perante nos ambientes virtuais seria através de cooperação internacional, motivo pelo qual foi redigido o Tratado de Budapeste, Atualmente, muitos países são signatários do mencionado tratado, entretanto, aparentemente por motivos de tradição diplomática, o Brasil, até o presente momento, não figura entre os signatários do mesmo. Ocorre que, nos últimos anos, notou-se uma crescente considerável de condutas altamente lesivas que vêm sendo praticadas através dos meios virtuais no país, que conta com uma legislação interna altamente desatualizada para efetivar a tutela de tais condutas nos meios digitais, resultando em uma grande gama de condutas altamente lesivas, porém atípicas. Dessa forma, pretende-se verificar se a adesão do Brasil à Convenção de Budapeste poderia auxiliar na efetivação da tutela estatal destas condutas lesivas.

PALAVRAS-CHAVE: Sociedade da Informação; Convenção de Budapeste; Crimes Virtuais; Cibercrime; Direito Digital.

ABSTRACT
This papper is related to the growing of the cybercrimes in Brazil and worldwide, demonstrating that the behaviors practiced with the use of virtual networks are becoming most visible in all the world. Knowing the fact that the virtual territory is a globally interconnected network who can be accessed simultaneously in various locations around the globe and can, as well, ignore the actual geopolitical borders, many countries have realized that the only way to exercise an

[1] Graduado em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas - FMU- SP (2018). Pós Graduado em Direito Penal e Criminologia pela Pontifícia Universidade Católica do Rio Grande do Sul - PUC-RS. Mestrando em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas FMU- SP

[2] Possui graduação em Ciências Jurídicas e Sociais pela Universidade Federal do Rio Grande do Sul (1999), mestrado em Direito pela Universidade Federal do Rio Grande do Sul (2001) e doutorado em Direito pela Universidade Federal do Rio Grande do Sul (2008). Coordenador do Mestrado em Direito da Sociedade da Informação no Centro Universitário das Faculdades Metropolitanas Unidas - Laureate International Universities. Professor da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul. Membro da Comissão Mundial de Direito Ambiental da União Internacional para Conservação da Natureza

effective judicial protection to all the users of this virtual world, would be through international cooperation policy, which is why the world's first cybercrime treaty was signed in the city of Budapest, in the year of 2001. The treaty is called Budapest Convention. By the way, at these days, many countries in the world are signed the treaty. Brazil, by the way, apparently for reasons of diplomatic tradition, is not among the signatories. In this way, it is intended to verify in what way Brazil's adherence to the Budapest Convention could assist in the effective state protection of these harmful conduct.

KEYWORDS: Information Society; Bodapest Convention; Virtual Crimes; Cybercrime; Digital Rights.

INTRODUÇÃO

O presente artigo pretende demonstrar que, diante da ineficácia atual da legislação brasileira no combate às práticas lesivas perpetradas pelos meios digitais, o ordenamento jurídico pátrio urge por inovações legislativas que sejam capazes de suprimir essa grave lacuna. Uma dessa inovações já vem sendo aplicada em diversos países, e poderia possivelmente auxiliar o Estado brasileiro a tutelar o meio ambiente digital de maneira mais eficaz. Trata-se da Convenção Internacional sobre o Cibercrime, ou simplesmente Convenção de Budapeste.

Muito embora a referida convenção venha apresentando resultados bastante favoráveis nos países onde foi implantada, o Estado brasileiro, mesmo atravessando uma crescente assustadora no número de pessoas lesadas pelos chamados de cibercrimes no país, não assinou o tratado. Além disso, a legislação interna do país evoluiu muito pouco nos últimos anos e vem se mostrando bastante incapaz de lidar com a problemática, como será demonstrado adiante do artigo. Também será demonstrado adiante que, salvo raras exceções, não se observa quaisquer mudanças significativas no ordenamento interno do país, no intuito de suprir a desatualizada legislação pátria vigente.

Fato que medidas urgentes são necessárias para que possa o Estado brasileiro exercer sua tutela jurisdicional nos ambientes digitais, sendo que a adesão ao tratado internacional de combate ao cibercrime seria uma solução rápida e que deteria um grau de eficácia já comprovada em outros países, entretanto, é necessário observar as peculiaridades específicas existentes na sociedade brasileira, e ponderar se as medias seriam realmente aplicáveis em um país cuja política criminal é seriamente controversa e ineficaz, como se verá adiante. No que se refere à metodologia de pesquisa, trata-se de um estudo bibliográfico com colheita de dados de modo qualitativo, principalmente, em um primeiro momento, estudos realizados por empresas de segurança da informação e doutrina específica voltada para a análise de ações perpetradas nos meios digitais.

1.A SOCIEDADE DA INFORMAÇÃO E OS CRIMES DIGITAIS NO BRASIL

Nota-se que, na maioria das localidades da terra onde existam sociedades humanas, ocorre, há muitos anos, uma verdadeira revolução social, econômica e cultural, que reordenou completamente os conceitos de fronteiras entre telecomunicações, meios de comunicação de massa e informática.

Nesse sentido explica Castells (2001, p. 21), ao apontar o final do século XX como um período em que foi possível vislumbrar acontecimentos sistêmicos que, quando analisados em sua amplitude, penetrabilidade e alcance social, poderiam ser caracterizados como uma verdadeira revolução, tais quais nossos antepassados atravessaram na Revolução Industrial e no Renascimento, porém, nestes tempos, a revolução tem por objeto central um bem completamente diferente: a informação. Tal objeto passou a ser reconhecido como um bem com total centralidade nas sociedades humanas, passando a fluir com velocidade e em quantidades antes inimagináveis, assumindo valores sociais e econômicos jamais antes considerados, ou seja, extremamente expressivos.

Conforme explica Barreto Jr.(2007, p. 2), convencionou-se nomear este novo ciclo histórico de Era da Informação, cuja mais distinta peculiaridade inerente às sociedades humanas vincula-se à existência de complexas redes profissionais e tecnológicas, voltadas à produção e ao uso da informação, que passa a ser considerado um bem valioso, utilizado para gerar conhecimento e riqueza.

E essas mudanças repentinas não se limitam unicamente à evolução tecnológica e à maneira que se dão as relações comerciais e econômicas entre as pessoas, mas incidem profundamente nas relações sociais. Nesse sentido explica Castells (2001, p. 22): “As mudanças sociais são tão drásticas quanto os processos de transformação tecnológica e econômica”. Ou seja, de maneira inequívoca, é possível notar a formatação de um novo sistema de comunicação em meio digital, global, que estabelece a interação em tempo real, além das redes interativas de computadores que crescem de forma exponencial, onde surgem novas formas e canais de comunicação que moldam as relações sociais e, simultaneamente, são moldados e formatados por estas.

Ocorre que, apesar destas irresistíveis mudanças sociais e tecnológicas terem trazido, à primeira vista, inúmeras benesses à dinâmica das relações sociais, comerciais e políticas que se sucedem entre os componentes de uma determinada sociedade, por outro lado, como descrito

no relatório da FADISP sobre o aumento dos crimes virtuais, realizado no ano de 2018, é notável também o surgimento de inúmeras novas possibilidades de pessoas mal-intencionadas obterem vantagens ilícitas ou praticarem atos lesivos e até mesmo criminosos de formas que antes não eram possíveis nem mesmo de se imaginar, utilizando-se tais agentes da possivelmente mais revolucionária das inovações tecnológicas desta e de todas as eras até então: a internet.

Conforme explica Crespo (2015), no ambiente *online*, pessoas são capazes de alimentar discursos racistas, fomentar o preconceito étnico e de gênero, divulgar propagandas de ódio e violência, alimentar os extremismos políticos e ideológicos, comprar e vender substâncias ilícitas na maioria dos países ocidentais, órgãos humanos, armas de fogo, roubar dados de pessoas físicas e jurídicas, incluindo dados bancários, invadir arquivos pessoais de pessoas comuns e de autoridades, praticar (com potencial lesivo antes nunca imaginado) crimes contra a honra, dentre outras inúmeras e lesivas ações capazes de causar sérios prejuízos a outras pessoas. Wendt e Jorge (2012) conceituam estas práticas, dizendo que, tais condutas, quando praticadas contra ou por intermédio de computadores, são denominadas como crimes cibernéticos.

Além disso, demonstra-se cada vez maior a pratica denominada *Fake news*, ora entendida, basicamente, como a difusão de informações falsas e distorcidas que, transitando de um lado a outro, é capaz de condicionar a opinião pública, tudo isso com muito pouca ou nenhuma capacidade do Estado de exercer sua tutela jurisdicional objetivando coibir a prática de condutas tipificadas como criminosas nestes meios digitais.

Como agravante deste problema, acresce-se o fato de que, nos meios virtuais, a criação das condições de possibilidade das ações criminosas geralmente é concebida/arquitetada por poucos indivíduos, que podem se valer (pessoalmente ou através de outros) de *modus operandi* matricialmente formatados para incontáveis situações lesivas e ilícitas. Em razão disto, como menciona Kist (2019, p. 61), a replicação de eventos delituosos virtuais – e suas vítimas - toma proporção quase que descontrolável.

Nos últimos anos, a prática destes crimes cibernéticos, também conhecidos como crimes digitais, apresentou franca ascensão em todo o mundo: segundo o mais novo relatório produzido por uma das maiores companhias de proteção à usuários de internet do mundo, a Symantec Norton Cyber Security, em 2018, mais de 978 milhões de pessoas em todo o mundo foram afetadas por *cybercrimes*, o que representa que 44% dos usuários de internet em todo o mundo já sofreram algum tipo de ataque virtual. Somente no que se refere de crimes

patrimoniais, as vítimas perderam a somatória de cerca de 172 bilhões de dólares para *cybercriminosos* ao redor do globo.

Assustadoramente, ainda segundo o relatório apresentado, o Brasil, que era em 2017 o 4º colocado da lista dos 20 países que mais sofreram com os *cybercrimes*, subiu duas colocações na lista, subindo para o atemorizante 2º lugar deste nefasto *ranking* no ano de 2018, atrás apenas da China, o que denota a importância de observar as causas e motivos desta imensa crescente que vem sendo experimentada.

Assim, evidente que se urge fomentar no Brasil, discussões acerca das melhores formas de inibir as condutas observadas e tidas por lesivas. Uma possível contribuição para a diminuição desta problemática seria uma modernização legislativa que fosse capaz de propiciar ao Estado melhores condições de exercer de maneira mais efetiva sua tutela jurisdicional nestes ambientes digitais, haja vista que, como mencionado por Bortot (2017, p. 349), o Brasil dispõe de uma legislação bastante parca no que se refere a condutas praticadas pelos meios digitais. Bortot (2017, p.350) destaca alguns raros exemplos de tipificações de condutas lesivas praticadas pelos meios digitais, dentre elas, a autora ressalta a Lei 12.735/12 e a Lei 12.737/12 – conhecidas como "Lei Azeredo" e "Lei Carolina Dieckmann", ambas criadas sob forte clamor popular momentâneo, diante de situações pontuais que haviam causado comoção social.

No Brasil, lamentavelmente, embora os debates nesta toada aparentem começar a ganhar fôlego, as únicas discussões levadas realmente à frente até este momento são àquelas onde as condutas lesivas praticadas nos meios digitais possam eventualmente gerar reflexos em questões relacionadas à assuntos envolvendo política e políticos[3], mantendo-se parcialmente inertes o legislativo e o executivo no que se refere ao grosso das condutas lesivas praticadas pelos meios digitais, ignorando o fato de que os crimes digitais vêm causando danos maciços à população brasileira, e que a legislação vigente não é adequada para que o Estado possa tutelar e combater de maneira efetiva estas cada vez mais frequentes condutas injustas.

Inacreditavelmente, a despeito de alguns órgãos estatais de grande relevância, como o Ministério Público Federal, já terem abertamente reconhecido a insuficiência da atual legislação penal brasileira no combate aos crimes digitais, e de defenderem amplamente, por exemplo, a adesão do Brasil a tratados internacionais voltados ao combate de condutas lesivas praticadas pelos meios digitais, em especial, a Convenção de Budapeste (MPF, 2019), o legislativo e o

[3] Por exemplo, em outubro de 2019, foi instaurada uma Comissão Parlamentar Mista de Inquérito para apurar a utilização de *Fake News* durante as eleições presidenciáveis de 2018. Disponível em: https://legis.senado.leg.br/comissoes/comissao?0&codcol=2292. Acesso em: 13 de nov. de 2019.

executivo, até o momento, não aparentam ter notado o potencial lesivo que pode ser alcançado pelos meios digitais, mantendo-se, portanto, inertes, apresentando até o momento, somente algumas medidas que vêm se mostrando completamente insuficientes para a adequação do ordenamento jurídico brasileiro aos novos tempos, permanecendo o Brasil desprovido de uma legislação moderna, que seja realmente eficaz em deter esta nefasta crescente de crimes cibernéticos que vitima a sociedade brasileira contemporânea.

Como se sabe, é papel do Estado, através do monopólio do Direito Penal, exercer a tutela dos bens jurídicos mais importantes aos seres humanos, aqueles considerados como fundamentais para a vida em sociedade (JESUS, 2014, p.46). E, de fato, resta evidente que as constantes condutas lesivas que vêm sendo perpetradas através das redes de internet extrapolam os interesses privados dos indivíduos, sendo urgente a intervenção do Estado, por meio do Direito Penal, a fim de exercer a tutela efetiva dos bens jurídicos tutelados pela Constituição Federal e por outras normas legais.

Tudo indica que a atual legislação processual penal no Brasil, encontra-se totalmente defasada no que se refere à tutela das condutas praticadas pelos meios digitais, sendo imperiosa e urgente a adoção de medidas que visem atualizar o ordenamento jurídico pátrio, a fim de tornar possível a prevenção e a punição das referidas condutas. Nesse sentido, explica com bastante acuidade Fuller (2014, p. 139), dizendo que "uma reconstrução da cultura do Direito Penal clássico se faz imperiosa em face dos delitos digitais que envolvem muitas cadeias relacionais e novas condutas praticadas no espaço virtual."

Assim, mostra-se evidente uma real ineficiência do atual *jus puniendi* estatal em face dos chamados crimes virtuais, ocasionado por vários fatores, mas o principal deles, se mostra a ligado à questão da defasagem legislativa a respeito dos chamados crimes digitais, sendo este um motivo mais que justificado para o Brasil passa a ratificar, por exemplo, o Tratado Internacional para enfrentamento dos crimes cibernéticos de Budapeste, que, como bem explicam Molitor e Velazquez (2017, p.94) detém o potencial de conduzir o Brasil a uma maior harmonização do ordenamento jurídico interno com o internacional, no que se refere ao combate à cibercriminalidade.

2.TRATADO INTERNACIONAL PARA ENFRENTAMENTO DOS CRIMES CIBERNÉTICOS: A Convenção de Budapeste.

Criada em 2001, a convenção sobre o cibercrime de Budapeste é o único tratado internacional sobre crimes cibernéticos, com normas de direito penal e processual penal, é voltado a definir estratégias conjuntas entre os países membros para a tipificação e o enfrentamento de crimes praticados na internet. Atualmente, segundo a lista disponibilizada pelo *Concil of* Europe (COI), conta com mais de 60 países signatários, sendo sua maioria membros da União Europeia, além de importantes membros de outros continentes, tais como Estados Unidos, Canada, Japão, além de países sul-americanos, como Colômbia, Argentina, Paraguai e Chile.

O referido tratado, foi elaborado em decorrência da percepção, por parte dos países signatários, da necessidade de cooperação internacional como condição para que seja possível coibir práticas ilícitas perpetradas nos ambientes digitais (CIDRÃO, MUNIZ e ALVEZ, 2018, p. 66/71), isso porque, como mencionado no capítulo anterior, o fenômeno da globalização e da popularização da Internet, relativizaram as fronteiras geopolíticas existentes até então, resultando num território comum entre os países, cenário em que se mostra absolutamente possível que alguém mal intencionado que esteja sob a tutela jurisdicional do Estado da Grécia cometa crimes que afetem cidadãos no Uruguai, por exemplo.

Além disso, Castells (2007, p.205) explica que "a internacionalização das atividades criminosas faz com que o crime organizado (...) estabeleça alianças estratégicas para cooperar com as transações pertinentes a cada organização, em vez de lutar entre si". Ou seja, a internet possibilitou que alguns dos crimes que já eram praticados no ambiente físico, passassem a ser praticados também no ambiente digital, e para piorar, de formas cada vez mais sofisticadas, podendo um único crime ser articulado por dois ou mais coautores de diferentes nacionalidades, situados em diferentes países.

Fernandes (2013, p.175) explica, de forma concisa, o principal objetivo da Convenção de Budapeste:

> O objetivo primário é a repressão dos crimes cibernéticos com a utilização de normas eficientes e práticas, mediante as quais a sociedade se sinta segura para se desenvolver, sem a interferência daqueles que procuram por meios escusos conseguir lucros, mesmo que causem prejuízos monetários e danos morais a terceiros

Dessa forma, como descrito em seu preâmbulo, a Convenção sobre o Cibercrime prioriza "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional" e reconhece "a necessidade de uma cooperação entre os

Estados e a indústria privada". Ressalta ainda, o obrigatório respeito por parte dos países signatários à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950), ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU (1966), à Convenção das Nações Unidas sobre os Direitos da Criança (1989) e à Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil (1999).

No que se refere a sua forma, o tratado possui quatro Capítulos (Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais, respectivamente) e 48 artigos, encorpados num texto didático e objetivo. Ressalte-se que, como bem observa Boiteux (2004), a convenção foi elaborada não somente para criar novos tipos penais, mas também para estipular normas de processo penal, conciliando procedimentos de direito penal internacional e estabelecendo acordos referentes à tecnologia da informação.

O instrumento inicia definindo conceitos e as terminologias adotadas no tratado. Em seu capítulo II, adentra a matéria de direito penal material, delimitando os cibercrimes, tipificando-os e separando-os em classes: infrações contra sistemas e dados informáticos; infrações relacionadas com computadores; infrações relacionadas com o conteúdo; pornografia infantil e infrações relacionadas com a violação de direitos autorais.

Nesta primeira parte, o tratado padroniza e tipifica algumas condutas notadamente lesivas, incitando os países signatários a adaptarem suas próprias legislações nacionais buscando criminalizar tais condutas[4]. Relevante ressaltar que no título 5, sugere-se[5] aos signatários que adotem as medidas legislativas cabíveis para que seja punível não somente os cibercrimes consumados, mas também sejam puníveis os crimes tentados. Outro ponto relevante acerca da matéria é o art. 12º, onde o tratado impõe à cada parte signatária que adote medidas cabíveis para responsabilização da pessoa jurídica por infrações cometidas por seus funcionários, quando estes encontrarem-se em posições de liderança na organização, podendo essa responsabilidade ser criminal, civil ou administrativa (ou todas elas), de acordo com ordenamento vigente do país signatário, sem prejuízo da responsabilidade criminal da pessoa física que cometeu a infração.

[4] A título exemplificativo, vide o art. 4º do referido acordo, que versa sobre a Interferência em Dados: "Artigo 4º - Interferência em dados - Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos".

[5] Aqui, ressalta-se o verbo "sugerir", uma vez que o artigo 11º, 3, é claro no sentido de que o signatário pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.º 2 do presente artigo.

A partir da seção 2, o tratado adentra nas questões relacionadas ao Direito Processual, e é aí que se encontra maior resistência por parte de alguns países, a exemplo do Brasil, para sua aderência. Isso porque, muito embora o art. 15º autorize adaptações na forma procedimental que se dará a aplicação do disposto, o tratado determina aos signatários que tais adaptações estejam de acordo com os princípios e com as convenções que o tratado menciona em seu preambulo, sobre o assunto, vale a leitura do mencionado artigo:

> Art. 15º - Condições e Salvaguardas. 1. Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma proteção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Proteção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das Nações Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade.

Ou seja, é preciso que o país signatário se adeque às referidas convenções para que cumpra devidamente a Convenção de Budapeste. Por fim, em suas disposições finais, ou seja, a partir do art. 36, a convenção dispõe acerca de sua aplicabilidade, vigência, efeitos, formas de adesão e reservas.

3.A APLICABILIDADE DA CONVENÇÃO DE BUDAPESTE NO COMBATE À CRIMINALIDADE DIGITAL NO BRASIL

Como se verificou, muito embora a convenção exija de seus membros que sigam alguns princípios fundamentais e regras estabelecidas em convenções anteriores, sua aplicabilidade é bastante relativizada, buscando amoldar-se de acordo com a legislação pátria de cada país signatário, objetivando, sobretudo, apontar caminhos e não propor soluções enrijecidas e únicas para a resolução dos problemas apontados, o que, em tese, facilitaria o ingresso do Brasil na adesão à referida convenção, mas até o presente momento, o país não aderiu ao tratado.

Cediço que, conforme dispõe o art. 37º da Convenção de Budapeste[6], o Brasil, por não ser um dos países que participaram da elaboração do tratado, demandaria receber um convite de um dos Estados membros para aderir à resolução, além de receber a aprovação unânime entre os demais Estados membros. Entretanto, isso não se mostraria difícil de acontecer, uma vez que as relações diplomáticas do país os países que atualmente compõe o grupo fundador são, neste momento, plenamente saudáveis.

Como mencionado anteriormente, o Ministério Público Federal, por reiteradas vezes já se manifestou no sentido de que a adesão seria vista com bons olhos e poderia auxiliar ao combate da criminalidade virtual no país, haja vista a falta de uma legislação moderna e específica para o combate dos cibercrimes no Brasil. Entretanto, até o presente momento, as discussões para o ingresso do país no mencionado tratado prosseguem, sendo que os apoiadores do ingresso do país no tratado continuam enfrentando grande resistência por parte do Itamaraty[7], em grande parte, acredita-se que, por conta da tradição diplomática brasileira de não aderir a acordos sobre os quais não foi sequer convidado a discutir os termos.

Em uma análise bastante resumida, é possível notar que a tipificação de algumas condutas, na forma realizada na Convenção, resta por ser um caminho que aparenta ser bastante coerente com os danos que vem sendo causados pelos criminosos virtuais. Nesse sentido, vale discorrer acerca do bem jurídico tutelado pela referida convenção.

O bem jurídico tutelado através da elaboração de normas que tipificam condutas ilícitas praticadas pelos meios digitais, como àquelas tipificadas na Convenção de Budapeste se trata de um bem jurídico de natureza difusa, nesse sentido explica Smanio (2000, p. 108):

> (...) trata-se de um bem jurídico-penal de natureza difusa. Isto porque, além de atingir um número indeterminado de pessoas, gera conflituosidade entre o interesse dos usuários da Internet, os hackers e os crackers, bem como das grandes corporações quer de fornecedores, quer de provedores de acesso.

[6] O referido art. 37 versa sobre as formas de adesão à Convenção, dispondo o seguinte: "(...) O Comitê de Ministros do Conselho da Europa pode(...) convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção"

[7] Nesse sentido: **Itamaraty ainda estuda adesão à Convenção de Budapeste**. Disponível em: https://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste. Acesso em: 21 de nov. de 2019 e **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e** Segurança. Disponível em: http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e seguranca-publica. Acesso em: 21 de nov. de 2019.

Para o mencionado autor, existem bens jurídico-penais individuais, dos quais se tem disponibilidade; bens de natureza coletiva, referentes à coletividade; e bens de natureza difusa, que, da mesma forma, referem-se à sociedade e são indisponíveis, porém com uma conflituosidade inerente a vários grupos sociais, notadamente meio ambiente, o consumidor e a saúde pública. Além disso, como explica Rossini (2004, p20), há um bem jurídico absolutamente permanente: a segurança da informática, independentemente dos bens jurídicos individuais ou coletivos.

Dessa forma, muito embora seja possível notar uma tímida evolução no ordenamento jurídico brasileiro na busca por tutelar condutas praticadas pelos meios virtuais, tais mudanças ainda são bastante insuficientes, não protegendo o bem jurídico tutelado em sua amplitude, e sim, outros bens jurídicos ou frações deles.

E a Convenção de Budapeste, além de possibilitar a tipificação de uma série de condutas lesivas praticadas pelos meios digitais, propicia uma forma hábil de enfrentar a problemática, pois, uma vez que as condutas lesivas abarcadas na convenção são cometidas no chamado ciberespaço, presume-se que o cibercriminoso tenha plenas condições de perpetrar suas ações ignorando as fronteiras geopolíticas vigentes, demandando um alinhamento entre os ordenamentos jurídicos existentes (CIDRÃO, MUNIZ e ALVEZ, 2018, p. 74).

A adoção da Convenção por parte do Brasil abarcaria a proteção legal e o combate de uma série de condutas que hoje não possuem qualquer previsão legal, como, por exemplo, a disposta no art.6º, *a*, da convenção, que determina como infração penal a produção de dispositivo ou programa informático, concebido para prática de infrações nos meios virtuais; ou a tipificada no art. 7º, que dispõe sobre a prática de falsidade informática. Evidentemente, tais tipificações seriam muito bem-vindas no ordenamento jurídico brasileiro, uma vez que tais condutas já vem sendo observadas corriqueiramente em território nacional, e causando severos prejuízos aos usuários, porém, em face de ausência de tipificação como práticas ilícitas, acabam por resultarem em condutas impuníveis. Como nos exemplos a seguir:

A reportagem veiculada em julho de 2019, pelo jornalista Victor Fuzeira (2019), descreve uma situação onde a Polícia Civil realizou a prisão de um casal acusado de integrar um grupo criminoso, pois em tese eles teriam sido responsáveis pela criação de um *software* utilizado para fraudar contas bancárias de terceiros. Muito embora o casal tenha sido preso preventivamente e aguarde o julgamento do feito, apesar de possivelmente serem condenados como incurso no art.2º da Lei 12.850/13 (organização criminosa), eles restarão, provavelmente, absolvidos pela prática de criar o referido *software* (embora respondam por outras acusações

também), pois, apesar de nitidamente uma conduta lesiva à sociedade, tal conduta carece de tipificação legal.

Outro exemplo de conduta lesiva que vem sendo praticada em massa e causando sérios prejuízos de ordem patrimonial e de ordem pessoal e que não encontra tipificação adequada na legislação brasileira é o famoso "golpe de clonagem de *whatsapp*", onde o cibercriminoso cadastra o número de telefone do usuário em outro dispositivo e, após esse processo, o usuário original recebe um SMS contendo um código de liberação de acesso.

Após o recebimento a vítima é induzida a fornecer esse código ao autor da prática e, em seguida, a sua conta de WhatsApp é bloqueada, momento no qual o autor começa a se passar pela vítima, geralmente pedindo dinheiro aos contatos da pessoa que teve seu *whatsapp* invadido, podendo inclusive, em certas situações, violar a privacidade da pessoa, tendo acesso à conversas, fotos, e outros documentos pessoais disponíveis no *software* de conversas[8]. Segundo levantamento divulgado pelo veículo jornalístico "Terra" (2020), tal prática tem tanta eficácia que, recentemente, em fevereiro de 2020, apurou-se que mais de 9 milhões de pessoas já caíram no referido golpe.

Entretanto, a ausência de tipicidade impede o combate efetivo à essas práticas, sendo muito comum a polícia somente instaurar investigação em casos onde seja possível aferir prejuízo financeiro de alguma das vítimas, enquadrando a conduta como delito de estelionato. Os danos à personalidade, ou as tentativas de estelionato acabam não sendo sequer investigados.

Ou seja, predomina o entendimento de que, se não houver prejuízo financeiro da pessoa que teve o número clonado, ou de seus contatos do aplicativo, não ocorrerá crime, pois o delito de estelionato exige um efetivo prejuízo para que seja configurado. Nesse sentido, os raros casos que ultrapassam a etapa pré-processual, e chegam ao poder judiciário, via de regra, implicam em absolvição, como nos precedentes abaixo:

> PENAL. PROCESSO PENAL. APELAÇÃO CRIMINAL. ESTELIONATO TENTADO. VÍTIMA NÃO ENGANADA. CONDENAÇÃO. IMPOSSIBILIDADE. ELEMENTO OBJETIVO DO TIPO NÃO CONFIGURADO. NÃO PROVIMENTO DO APELO. 1. Quando o meio fraudulento empregado não é capaz de enganar a vítima, não há falar em prática do delito de estelionato, uma vez que os atos praticados foram meramente preparatórios. 2. Constatado que a vítima não fora ludibriada pelos réus e que tinha plena ciência do 'golpe' que estaria sofrendo, imperiosa é a

[8] Vide um exemplo típico *do modus* operandi do chamado golpe do whatsapp: https://tribunademinas.com.br/noticias/cidade/29-04-2019/policia-civil-alerta-para-golpe-de-clonagem-do-whatsapp.html

> absolvição, levando-se em conta que não resta configurado um dos elementos objetivos do tipo penal.
>
> (TJ-AC - APL: 00007836320158010001 AC 0000783-63.2015.8.01.0001, Relator: Des. Pedro Ranzi, Data de Julgamento: 25/04/2017, Câmara Criminal, Data de Publicação: 26/04/2017)
>
> PENAL. APELAÇÃO CRIMINAL. ARTIGO 171, CAPUT, E ARTIGO 168, § 1º, INCISO III, NA FORMA DO ART. 69, TODOS DO CÓDIGO PENAL. ESTELIONATO - AUSÊNCIA DE PREJUÍZO ALHEIO - ABSOLVIÇÃO - POSSIBILIDADE. (...)Necessário para o decreto condenatório relativo ao crime de estelionato a demonstração efetiva do prejuízo decorrente da ação criminosa (...)
>
> (TJ-DF 20150110220662 0006286-97.2015.8.07.0001, Relator: ROMÃO C. OLIVEIRA, Data de Julgamento: 27/04/2017, 1ª TURMA CRIMINAL, Data de Publicação: Publicado no DJE : 04/05/2017 . Pág.: 399/419)

Dessa forma, essa tentativa de aplicar a conduta tipificada pelo legislador no art. 171 do Código Penal na situação presente (golpe via *whatsapp*) se mostra deveras ineficaz, pois não criminaliza a conduta que antecede o prejuízo financeiro, a qual por si só já viola gravemente a privacidade da vítima. A impunidade nestes casos, reside na ausência da tipificação específica da referida conduta. Como no exemplo anterior, a Convenção de Budapeste também poderia auxiliar no combate à essas práticas, pois tipifica, em seu art. 7º, exatamente a conduta que vem sendo praticada pelos fraudadores, cabendo somente ao ordenamento brasileiro determinar a pena a ser cominada.

De toda forma, as condutas supramencionadas são somente duas situações, entre diversas outras que vêm sendo observadas e que poderiam ser relatadas no presente artigo. Mas o que realmente importa demonstrar na presente ocasião é o fato de que resta evidente que a legislação atual no país não está apta para inibir os cibercrimes, sendo esta defasagem legislativa o provável motivo principal para justificar a crescente desta modalidade de condutas lesivas no país. Corroborando com este entendimento, está o fato trazido pelo mencionado relatório da Symantec, que menciona que os dois países que mais sofreram com os cibercrimes no último ano (Brasil e China), não são signatários da convenção de Budapeste, será uma coincidência?

A adesão do Brasil ao tratado parece ser uma excelente saída para a defasagem legislativa que paira sobre a problemática, uma vez que a alternativa seria a elaboração de um ordenamento jurídico próprio, o que parece a solução mais difícil, haja vista a extrema polarização política e de ideias se nota no país, e em especial no poder legislativo nestes tempos. A adequação da legislação ao tratado, além de ser possível, seria possivelmente uma transição

relativamente célere, uma vez que dezenas de outros países já fizeram a mesma adequação, não sendo, portanto, um caminho desconhecido a ser percorrido.

A única problemática que se observaria com a aderência ao tratado (e que demandaria um estudo maior e mais aprofundado acerca de suas consequências) relaciona-se com uma outra questão tormentosa que faz parte da realidade na política criminal brasileira: a política do encarceramento em massa.

Como se sabe, segundo o mais recente Levantamento Nacional de Informações Penitenciárias, a população carcerária no Brasil está em franca ascensão, tendo ultrapassado a assustadora marca de mais de 700 mil presos em 2019, sem que de fato tenha uma redução significativa nos índices de criminalidade, o que, aliado a outros fatores, demonstra uma falência do sistema penal brasileiro, além de uma séria ineficácia em prevenir novas práticas delitivas no país. De toda forma, essa questão não deveria se situar como um empecilho para a adoção do referido tratado.

Isso porque, como se nota na Convenção, em seu art. 13º, o tratado instrui a seus signatários a possibilidade de adotarem medidas que se revelem necessárias para assegurar que as condutas tipificadas como criminosas no capítulo 02, recebam as sanções de adequadas, de acordo com a realidade e a necessidade de cada país. Ou seja, significa que o Brasil poderia sim utilizar-se da Convenção para criminalizar as condutas sem agravar a caótica situação de seu sistema prisional, bastaria que fossem adotadas sanções modernas, que buscassem coibir de maneira inteligente novas práticas delitivas, o que por certo, a pena de reclusão não faz (ao menos no Brasil).

Desse modo, embora a convenção determine que as mencionadas condutas sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas da liberdade, na realidade fática brasileira, a privação de liberdade deve ser combativamente evitada, pois dificilmente demonstraria ser efetiva no caótico cenário brasileiro, que, além de possuir uma previsão assombrosa no que se refere ao crescimento da população carcerária, possui um dos maiores índices de reincidência do mundo, que por sinal não param de crescer.

Assim, dada a atual conjectura, qualquer política pública que incentive o ultrapassado modelo punitivista de privação de liberdade vigente no país deve ser evitada, sendo, portanto, imperiosa a observância, em caso de adesão ao tratado, do consagrado princípio do direito penal de *ultima ratio* e, nos casos onde se mostrar necessária a aplicação do Direito Penal, cumpre dispender especial atenção à necessidade de imposição de medidas penais alternativas ao encarceramento.

CONCLUSÃO

Ante o exposto, é possível concluir que o momento vivenciado pela maioria das sociedades contemporâneas é extremamente delicado e de transição, decorrente, em especial, da revolução tecnológica que se vislumbra na presente Sociedade da Informação. Com a popularização da *internet*, pôde-se observar que um novo território foi criado, e neste território as relações humanas se dão de maneiras antes jamais imaginadas. E estas mudanças se deram de forma tão abrupta e repentina, que foi possível notar que os Estados, em sua maioria, demonstraram uma imensa dificuldade de exercer sua tutela jurisdicional para regular e controlar as condutas perpetradas no ambiente virtual.

E tal ineficácia por parte do Estado não passou desapercebida, em especial no Brasil, por um número cada vez maior de agentes mal intencionados que utilizam-se das condições singulares que são propiciadas pela *internet* para praticar condutas altamente lesivas, muitas vezes criminosas, tais como fraudes, estelionatos virtuais, roubo de dados, invasão de dispositivos alheios, crimes contra a honra com potencial imensurável, estupros virtuais, deflagração de *fake News*, e muitas outras condutas altamente problemáticas para a ordem pública e para a sociedade como um todo.

Agravando esta situação, como a *internet* se trata de uma rede mundial de computadores, não é inabitual que estas práticas criminosas sobrepujem as fronteiras geopolíticas tradicionais, causando ainda maior confusão na efetivação de investigações e na aplicação de sansões contra os agentes, isso porque, cada país conta com uma legislação específica para o combate deste tipo de crime, e outros, como o Brasil, conta com um fraco aparato técnico investigativo e legislativo para enfrentar e controlar estas práticas tidas como lesivas.

Notando este cenário belisário, foi adotado pelo Comitê de Ministros do Conselho da Europa, na sessão 109 de 08 de novembro de 2001, a Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste, onde uma série de países europeus elaboraram regras gerais para facilitar o combate às práticas lesivas perpetradas nos ambientes digitais, tipificando as principais condutas, e sugerindo formas de cooperação internacional no combate destas ações. Apesar de ter sido firmado por países membros do Comitê Europeu, é plenamente

possível a adesão dos demais países do mundo no tratado, contanto que exista um convite feito pelos países originalmente signatários.

Pensando justamente nesta heterogeneidade de legislações, o tratado busca definir critérios maleáveis, sem a rigidez de outros tratados internacionais, exatamente para ser possível a adesão da maior parte de países, o que acarretaria uma maior cooperação internacional na repressão às condutas tipificadas no artigo. Além disso, como explicam Bechara e Flores (2019) , a conduta criminosa, quando praticada pelos meios virtuais, extrapola fronteiras, causando problemas com relação à competência territorial dos Estados-Nação. Ou seja, mais um motivo para formalizar institutos de cooperação internacional como a Convenção de Budapeste.

Eventualmente, diversos países foram aderindo ao tratado e modelando seus sistemas jurídicos para efetivar sua aplicação, outros aderiram parcialmente, complementando gradativamente suas próprias legislações pátrias conforme seus interesses e ditames nacionais.

O Brasil, entretanto, não aderiu à Convenção, e tampouco demonstrou até o momento dar a devida importância para propiciar à seus nacionais uma maior segurança para a navegação nos meios digitais, sendo possível notar algumas tímidas mudanças legislativas nos últimos anos, mas nada substancial, que detenha aptidão suficiente para substituir a efetividade da Convenção de Budapeste. Este é o principal motivo, como demonstrado no início do presente artigo, do Brasil ter subido duas posições no ranking de países que mais sofrem com cibercrimes, ostentando o segundo lugar dentre os países que mais sofreram com os crimes virtuais, segundo a empresa Norton Cyber Security.

Por este motivo, alguns órgãos de grande relevância, como o Ministério Público Federal, se manifestaram abertamente pela adesão do país ao tratado, o que certamente seria benéfico e contribuiria para propiciar melhor segurança para as empresas e pessoas físicas que diariamente utilizam-se dos meios digitais em suas mais variadas relações econômicas e sociais.

Recentemente, diante da crescente pressão dos órgãos persecutórios, o governo federal deu singelos passos no sentido de aderir ao tratado, tendo se manifestado o Ministério da Justiça, em sentido favorável adesão ao tratado, com base em relatórios da Polícia Federal e do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), o que se espera que possa indicar caminhos promissores na efetivação da tutela jurisdicional estatal em face das condutas praticadas nos meios digitais.

Cumpre salientar que, no caso de o Brasil finalmente tornar-se signatário da Convenção de Budapeste, o tratado menciona que cada país signatário deverá aplicar sanções eficazes para as condutas lesivas tipificadas na convenção. Ressalte-se que esta problemática

merece especial atenção no Brasil, pois é possível verificar, devido à atual situação político-social que atualmente atravessa o país, a predominância de uma prática Estatal notadamente punitivista de encarceramento em massa, o que já resulta em mais de 700.000 (setecentas mil) pessoas privadas de sua liberdade, com projeções de crescimento assustadoras.

Uma vez que tal aumento das prisões não vem demonstrando eficácia na diminuição da criminalidade, tampouco nos índices de reincidência (que permanecem como um dos maiores do mundo), é imperioso que as eventuais sanções para os crimes digitais detenham um caráter moderno e eficaz, não bastando ao Estado limitar-se a aplicar as ultrapassadas políticas de combate à criminalidade atualmente utilizadas (que se resumem, basicamente, na privação da liberdade do indivíduo) e esperar que o caráter retributivo da pena seja suficiente para apaziguar a criminalidade digital no Brasil.

Ademais, como muito bem exposto por Klymenko, Gustalyuk e Savchenko, (2020, p.27), além de uma legislação moderna para tornar possível o enfretamento da problemática, também é imperiosa a criação de unidades estruturais especializadas nos entes estatais responsáveis pela fase investigatória e de construção probatória (Polícia Judiciária e Ministério Público por exemplo), para tornar possível a aplicação prática das normas porventura tipificadas.

REFERÊNCIAS

BARRETO JUNIOR, Irineu Francisco. Atualidade do Conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi (coord.). **O Direito na Sociedade da Informação**. São Paulo: Atlas, 2007

BRASIL. TJDF – Apelação n.: 20150110220662 0006286-97.2015.8.07.0001. Relator: Romão C. Oliveira. Data de Julgamento: 27/04/2017, 1ª TURMA CRIMINAL, Data de Publicação: Data de Publicação: 04/05/2017. p. 399/419.

BRASIL. TJAC – Apelação n.: 00007836320158010001 AC 0000783-63.2015.8.01.0001. Relator: Des. Pedro Ranzi, Data de Julgamento: 25/04/2017, Câmara Criminal, Data de Publicação: 26/04/2017. p. 324/411.

BECHARA, Fábio Ramazzini; FLORES, Dimitri Molina. Crimes cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional?. Revista Direito Mackenzie. São Paulo, v. 13, n.2, p.1-21, 2019.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. In: **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004.

BORTOT, Jessica Fagundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **Revista VirtuaJus.** Belo Horizonte, v. 2, n.2, p. 338-362, 2017.

CASTELLS, Manuel. **A Era da Informação: economia, sociedade e cultura.** Volume I, a sociedade em rede. 5. ed., São Paulo: Paz e Terra, 2001.

CASTELLS, Manuel. **Fim do Milênio**. 4. ed., São Paulo: Paz e Terra, 2007.

CIDRÃO, Taís Vasconcelos; MUNIZ, Antônio Walber; ALVES, Ana Abigail Costa Vasconcelos. **A oportuna e necessária aplicação do direito internacional nos ciberespaços: da Convenção de Budapeste à legislação brasileira**. *In*: Brazilian Journal of International Relation, Marília, v. 7, ed.1, 2018, p. 66-82.

Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Acesso em: 12 de nov. 2019.

CNJ registra pelo menos 812 mil presos no país; 41,5% não têm condenação. Disponível em: https://g1.globo.com/politica/noticia/2019/07/17/cnj-registra-pelo-menos-812-mil-presos-no-pais-415percent-nao-tem-condenacao.ghtml. Acesso em: 21 de nov. de 2019.

CPMI das Fake News. Disponível em: https://legis.senado.leg.br/comissoes/comissao?0&codcol=2292. Acesso em: 13 de nov. de 2019.

Convenção de Budapeste. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 13 de nov. de 2019.

CRESPO, Marcelo. **Deep Web: o submundo do crime**. Canal Ciências Criminais, 2015. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/noticias/211380741/deep-web-o-submundo-do-crime. Acesso em: 17 de abr. de 2020.

Estudo mostra que maioria dos que deixam prisão voltam para o crime. Disponível em: https://www.em.com.br/app/noticia/gerais/2017/09/30/interna_gerais,904836/estudo-mostra-que-maioriados-que-deixam-prisao-voltam-para-o-crime.shtml. Acesso em: 21 de nov. de 2019.

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. **Revista da Faculdade de Direito da UFMG**. Belo Horizonte, n.62, p.139-178, jan/jun. 2013.

FULLER, Greice Patrícia. **O Direito Criminal Difuso, a dignidade da pessoa humana e a mídia na Sociedade da Informação**. In: Anais do VII Congresso Brasileiro da Sociedade da Informação – Regulação da Mídia na Sociedade da Informação: São Paulo, 2014, p. 131-141.

FUZEIRA, Victor. **Casal usava programa para fraudar contas de clientes de bancos.** Disponível em: https://www.metropoles.com/distrito-federal/df-casal-usava-programa-para-fraudar-contas-de-clientes-de-bancos. Acesso em: 15 de fev. 2020.

Itamaraty ainda estuda adesão à Convenção de Budapeste. Disponível em: https://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste. Acesso em: 21 nov. de 2019.

JESUS, Damásio de. **Direito Penal, volume I: parte geral. 35. ed. São Paulo: Saraiva, 2014.**

KLYMENKO, Olga A.; GUTSALIUK, Mykhailo V.; SAVCHENKO, Andrii V. Combater o cibercrime como pré-requisito para o desenvolvimento da sociedade digital. JANUS.NET ejournal of International Relations, v.11, n. 1, mai/out. 2020. Disponível em: https://repositorio.ual.pt/handle/11144/4542. Acesso em: 28 jul. 2020.

KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019

MOLITOR, Heloísa Augusta Vieira; VELAZQUEZ, Victor Hugo Tejerina. Breve panorama sobre a legislação aplicada nos crimes eletrônicos. **Revista de Direito, Governança e Novas Tecnologias**. Maranhão, v.3, n.2, p.81-96, jul./dez. 2017.

MPF defende adesão do Brasil à Convenção de Budapeste em audiência pública na Câmara. Junho de 2019. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/mpf-defende-adesao-do-brasil-a-convencao-de-budapeste-em-audiencia-publica-na-camara. Acesso em: 6 de jun. de 2019.

Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Disponível em: http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 22 de mar. de 2020.

Relatório da Symatec Norton Cyber Security. Disponível em: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf. Acesso em 13 de nov. de 2019.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SMANIO, Gianpaolo Poggio. **Tutela penal dos direitos difusos.** São Paulo: Atlas, 2000. p. 108.

TERRA. **Golpe do *Whatsapp* faz mais quase 9 milhões de vítimas no Brasil.** 2020. Disponível em: https://www.terra.com.br/noticias/dino/golpe-do-whatsapp-clonado-ja-fez-quase-9-milhoes-de-vitimas-no brasil,4e8c58dea39ba313f825b72d38afe589ylmm1z4t.html. Acesso em: 23 de mar. de 2020.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012.