JURISDIÇÃO CRIMINAL E DELITOS INFORMÁTICOS: REFLEXOS NA JURISDIÇÃO BRASILEIRA DA CONVENÇÃO DE BUDAPESTE

CRIMINAL JURISDICTION AND IT OFFENSES: REFLECTIONS IN THE BRAZILIAN JURISDICTION OF THE BUDAPEST CONVENTION

Felipe Pinheiro Prestes[1]

Elvis Preis Anacleto[2]

RESUMO

O presente estudo se trata de uma pesquisa em andamento que tem por finalidade abordar a forma que a legislação brasileira trata os delitos informáticos, mais precisamente em relação a jurisdição criminal no ciberespaço. Em um primeiro momento, passa-se a tentativa de correta conceituação dos delitos praticados por meio da rede mundial de computadores. Logo, é abordado a problemática relacionada a jurisdição criminal relacionada à problemática da jurisdição criminal no ciberespaço. Por fim, analisa-se a Convenção de Budapeste de 2001, único tratado internacional que tenta homogeneizar as legislações dos países a fim de combater os delitos informáticos, trazendo inclusive formas de dirimir questões que tratam de conflito de jurisdições – ponto focal da presente abordagem. Nesta pesquisa, foi adotada a metodologia exploratória e descritiva documental, em conjunto com o método hipotético-dedutivo. Como resultado, evidencia-se que existe um déficit de alcance da convenção no cenário interno brasileiro, mesmo após ter iniciado o processo adotar a norma para dentro do território nacional, o que faz permanecer o caráter de falta de segurança jurídica sobre o tema.

Palavras-chave: Convenção de Budapeste; Delitos informáticos; Jurisdição.

ABSTRACT

The present study is ongoing research that aims to address the way in which Brazilian legislation treats computer crimes, more precisely in relation to criminal jurisdiction in cyberspace. Firstly, there is an attempt to correctly conceptualize the crimes committed through the world wide web. Therefore, the issue related to criminal jurisdiction is addressed in relation to the issue of criminal jurisdiction in cyberspace. Finally, the

[1] Mestrando em Direito, Universidade do Extremo Sul Catarinense. E-mail: felipepresters@gmail.com.
[2] Graduando em Direito, Universidade do Extremo Sul Catarinense. E-mail: elvispreis@outlook.com.

2001 Budapest Convention is analyzed, the only international treaty that attempts to homogenize the laws of countries to combat computer crimes, including ways of resolving issues that deal with conflict of jurisdictions – the focal point of this approach. In this research, the exploratory and descriptive documentary methodology was adopted, together with the hypothetical-deductive method. As a result, it is evident that there is a deficit in the scope of the convention in the Brazilian domestic scenario, even after having started the process of adopting the norm within the national territory, which means that there remains a lack of legal certainty on the subject.

Keywords: Budapest Convention; Computer crimes; Jurisdiction.

1. INTRODUÇÃO

O conflito jurisdicional representa aspecto reconhecidamente importante em relação a legitimidade de um Estado para se declarar competente para conhecer determinado delito que possa alcançar e prejudicar o cidadão, assim como bem jurídico tutelado desse, que se encontram sob a sua soberania legislativa e territorial.

Por esse aspecto, primeiramente deve ser observado que há séculos o entendimento do sistema de Vestfália tem permanecido entre os Estado-nação. O que significa dizer que, cada país possui soberania estatal dentro do seu território, caráter que impeditivo para que autoridades externas se intrometam em questões e assuntos que sejam tão e somente internos. A estrutura segue preservada nos moldes legais atuais, garantida e preservada por um sistema de fronteiras geograficamente demarcadas, exércitos e armas as guarnecendo, que são meios de controle a fim de limitar imigração e emigração territorial. Contudo, essa estrutura se mostra deficitária em relação ao processamento de delitos que são cometidos por meio da Rede Mundial de Computadores, visto que não são limitados por fronteiras geográficas.

Por consequência, é necessário investigar se há ou pode haver instrumento jurídico que facilite a persecução e produção de provas de delitos informáticos, a fim de garantir proteção ao cidadão independente das características desses crimes.

Por anto, o presente trabalho abordará ao final a Convenção de Budapeste de 2001, tratado que tenta homogeneizar as legislações dos países membros sobre a temática, bem como a eficácia e influencia quem tem na legislação brasileira, se for o caso.

2. OS DELITOS INFORMÁTICOS

É possível conceituar o crime informático como o fato típico e antijurídico cometido envolvendo o uso de tecnologia – como dispositivos eletrônicos diversos conectados à web, entre eles: computadores, smartphones, tablets – contra um sistema, dispositivos informáticos diversos, contra rede de computadores ou então, em desfavor de indivíduos (Barreto; Brasil, 2016, p. 43). Ainda, pode ser dito como toda conduta que atente contra o processamento, armazenamento e transmissão de dados, explorando as fragilidades dos sistemas que integram a complexidade da rede mundial de computadores (Martín, 2012, p. 781-799). Ademais, destaca-se afirmando, que no crime cibernético, a informática pode ser o bem ofendido ou então o meio a fim de cometer ofensas aos bens jurídicos tutelados pelo Direito Penal (Martín, 2012, p.781-799).

Outrossim, legalmente, conforme conceitua a legislação internacional específica - referindo-se à Convenção de Budapeste que será estudada detalhadamente no momento que for tratado da jurisdição processual penal dos delitos informáticos, que por sua vez foi embasada pelo Conselho da Europa define mais adequadamente como a ação como os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas de redes e dados informáticos, além de poder ser a ação contra o correto funcionamento das Redes (Conselho da Europa, 2001).

Nesse mesmo sentido, a doutrina de WENDT e JORGE (2013, p. 19-29) distinguem as condutas criminosas entre crimes cibernéticos e ações prejudiciais atípicas, sendo que o primeiro se divide em mais duas categorias, quais sejam, crimes cibernéticos abertos – delitos que podem ser praticados de forma tradicional, ou seja, sem a necessidade de um computador, contudo, podendo-se também utilizá-los, caracterizando-se, dessa forma, como uma conduta-meio. Por outro lado, quando se tratando de crimes exclusivamente cibernéticos, figura-se ações atos criminosos que só podem ser perfectibilizados por meio de sistemas tecnológicos que permitam o acesso à Internet, tutelando a inviolabilidade dos dados – como exemplo, a tipificação

contida no já citado artigo 154-A do Código Penal, ou então, o artigo 241-D do Estatuto da Criança e do Adolescente (Brasil, 1990).

Ademais, as ações prejudiciais atípicas não se caracterizam como crimes informáticos, pois se trata das condutas praticadas utilizando-se da web, causando algum transtorno à vítima, porém, sem previsão legal na legislação criminal, são invasões computacionais obstinadas que, em que pese tragam intempéries à vítima, não serão indiciadas criminalmente, contudo, podem ser objeto de ações cíveis de reparação de danos materiais e morais (Wendt; Jorge, p.19).

Outrossim, pode ocorrer a fusão de tais classificações, haja vista que pode um agente cometer delito em que um bem jurídico informático seja agredido para que ele possa perfectibilizar um crime-fim, ou seja, agredir bem informático tutelado com a intenção de causar mal a outro bem, mesmo que não digital (Jesus; Milagre, 2016, p. 53).

Não obstante, GUARAGNI e RIOS (2019, p.175-176) classificam os delitos informáticos de forma análoga, quando os divide em duas classificações, quais sejam, impróprios e próprios. Em relação ao impróprios, são aqueles cometidos utilizando-se de meios informáticos de dados, da mesma forma que o crimes cibernéticos abertos de WENDT (p. 19-20), são ações tipificadas que necessariamente não necessitam meio digital para serem perpetradas, bem como atingem bem jurídicos diversos e corriqueiramente tradicionais, portanto, podem ser crimes comuns que foram praticados na web. Os crimes digitais próprios, são atos típicos nos quais o bem jurídico o bem jurídico podem ser a inviolabilidade das informações automatizadas, ou seja, os dados, contudo, conforme doutrina, o atinge no mínimo em três dimensões, sendo elas, a privacidade – inviolabilidade de dados – a acessibilidade ou disponibilidade de dados e a transparência e veracidade dos dados, os quais conjuntamente concretizam-se na seguridade informática, enquanto bem jurídico, se tratando de delitos que surgem e encontram formas de crescimento junto com o advento da Internet (Guaragni; Rios, p. 178).

Por outro lado, segundo apontamento de MARTÍN (2012, p. 1.105-1.115), o departamento de justiça estadunidense utiliza outra forma de nomenclatura para os delitos cibernéticos a depender da ação praticada em um equipamento informático, a

primeira está relacionada a máquina como sendo o objeto do crime, estes que fazem parte de um rol já penalizados pela legislação, onde se insere o roubo de software e hardware. Já a segunda classificação, na qual se encaixam as demais condutas delituosas por meio da web, informa que sistema informático se trata do sujeito do crime, não existindo analogias a demais crimes já penalizados da mesma forma que a primeira classificação.

Destarte, conforme JESUS e MILAGRE (2016, p. 53-54), pode-se classificar os delitos informáticos em quatro diferentes classificações, quais sejam, crimes informáticos próprios, crimes informáticos impróprios, crimes informáticos mistos, crime informático mediato ou indireto.

Os crimes informáticos próprios, especialmente relevantes no estudo em questão, são caracterizados pelo fato de que o bem jurídico tutelado se trata da informação em si, ou seja, a norma protege a inviolabilidade das informações automatizadas, os dados (Viana; Machado, 2013, p. 32-33), observa-se que para essa espécie a legislação penal era lacunosa, uma vez que muitas ações não poderiam ser enquadradas criminalmente, porém conforme se molda o presente estudo até então, mostra-se que já existem tipificações próprias no sistema jurídico pátrio, por exemplo o já referenciado artigo 154-A do Código Penal (Wendt; Jorge, 2013, p. 19-20.), bem como a interceptação ilegal de dados, o qual foi positivado pelo artigo 10º da Lei nº 9.296/1996 (Brasil, 1996).

Em relação aos crimes informáticos impróprios, são os delitos em que um equipamento com acesso à *internet*, é utilizado como instrumento para executar o crime, sem que exista ofensa a bem jurídico informático. São atos de grande popularidade que não exigem grande conhecimento computacional para o cometimento do ato ilícito. Os clássicos exemplos desta forma criminosa são os delitos contra a honra, contudo pode ser citado a instigação ao suicídio, o estelionato, violação de segredo profissional, apologia ao crime, dentre outros. Em síntese, são crimes que podem ser cometidos fora do âmbito digital (Viana; Machado, p. 30-31).

Quantos aos delitos informáticos mistos, são ações criminosas onde se identifica mais de um tipo penal, atingindo mais de um bem jurídico (Jesus; Milagre, p. 54.). A doutrina ainda aponta que são delitos derivados da invasão de dispositivo

informático, e dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos, ganharam o status de crimes sui generis (Viana; Machado, p. 34-35).

Sobre crime informático mediato ou indireto, a doutrina destaca que o delito informático é praticado para que um crime-fim não informático seja consumado, geralmente de ordem patrimonial, como exemplo, a captura de dados bancários para que sejam utilizados para desfalcar a conta corrente da vítima, sendo que o agente será punido somente pelo furto, neste caso o crime-fim, o que se dá devido a aplicação do Princípio da Consumação, seria a forma de dizer que o delito final herdou a características do delito informático que possibilitou a sua perfectibilizarão (Viana; Machado, 2013, p. 35-36).

Por óbvio a última classificação de delito informático parece se confundir com as duas que o antecederam. Porém o delito informático mediato não se confunde com o impróprio, isto porque, no primeiro há lesão do direito à inviolabilidade dos dados informáticos, mesmo que não penalizado devido a incidência do Princípio da Consumação. Da mesma forma, não se confunde o crime informático mediato com o misto, pois neste, há dois tipos penais protegendo diferentes direitos autônomos (Viana; Machado, 2013, p. 36).

Dessa forma, possível perceber que em que pese existam diferentes nomenclaturas para esses delitos, todos utilizam de alguma forma a Rede Mundial de Computadores, podendo ser ações praticadas de um Estado e gerando os resultados em outro, razão pela qual se tem a necessidade da presente pesquisa avaliar possível instrumento jurídico que possa auxiliar na persecução penal e futuro processo independente do local de origem do delito.

3. O CIBERESPAÇO E A PROBLEMÁTICA DA JURSIDIÇÃO CRIMINAL

A Internet é uma rede de alcance mundial formada por um conjunto de dispositivos, sendo que no território da *web* estão disponíveis diversos serviços que dão acesso as informações disponibilizadas por sites acessáveis por mecanismos de buscas, cobrindo, praticamente, todas as áreas dos interesses sociais dentre eles

existem redes sociais, e-commerce e serviços de mensagens eletrônicas (Leonardi, 2005, p. 13).

Assim, pode-se afirmar que a partir do nascimento da *World Wide Web*, surge um espaço de comunicação aberta, interconectando mundialmente de forma sinérgica computadores e memórias informáticas o que acabou por ser chamado de ciberespaço, conforme conceitua Levy (Levy; Costa, 1999, p. 92), ambiente responsável pela transmissão internacional de dados informáticos, termo este que surgiu do romance ficcional no ano de 1984 intitulado de Neuromancer, escrito por Wiliam Gibson (2016, p.25). Outrossim, não fora necessário longos anos para que aparecessem sujeitos que descobriram fraquezas nos sistemas de troca de dados por meio do ciberespaço, assim, explorando-as surgiu uma nova espécie de delito, figurando uma nova ameaça à sociedade informacional, responsável por uma lucrativa prática criminosa que desafia o novos operadores do direito preocupados com atos com baixa taxa de persecução penal frente aos desafios intrínsecos a questão, em especial o Estado com jurisdição responsável pela investigação e pelo julgamento do criminoso, tem que será cuidadosamente analisado pelos parágrafos seguintes.

Os responsáveis por essa espécie de prática criminosa podem ser classificados como *crackers* ou alguém desprovido de notório conhecimento informático de programação computacional se valendo do pouco conhecimento de alta porcentagem dos usuários dos serviços disponibilizados no Rede, seja lazer ou a negócios, ou então alguém que se utilize de Engenharia Social para levar induzir a vítima a erro. Nesse sentido, a figura que de fato mais mitologia se constrói se trata do *cracker*, que erroneamente como já citado é chamado de *hacker*. Sujeito que não nasce, mas sim é criado no submundo informático e apoiado por enorme quantidade de material disponível e redes de compartilhamento (Goodman, 2016, p. 25).

Por outro lado, faz-se necessário explanar sobre a dificuldade na persecução penal para a localização e julgamento de um *craker*, uma vez que, como sustentado, a prática das atividades delitivas se dá por meio da complexidade da rede em escala mundial classificada de ciberespaço (Martín, 2012, p. 530).

Em que pese esse espaço não seja corpóreo, físico ou abranger espaço geográfico tangível, bem como aparentar se tratar de uma rede etérea, na verdade é uma representação e construção social à imagem e semelhança do mundo físico. Assim, para correto funcionamento da transmissão de informação, faz-se necessário obedecer a critérios matemáticos organizacionais, a fim de permitir a correta fluidez dos sistemas, processo que se dá por meio dos servidores, espaços físicos de responsabilidade de empresas encarregadas pelo armazenamento, endereçamento e processamento de toda a espécie de informação disponível na Rede, obrigadas a obedecer determinadas legislações. São essas informações que se caracterizam como sendo as provas digitais, assim como os cookies, que podem ser caracterizados como indícios da atividade criminosa deixados no dispositivo da vítima que fora invadido com elas é possível elucidar crime real (Shimabukuro, 2017, p. 20).

Ademais, insta salientar que a partir destas é possível chegar ao verdadeiro paradeiro do sujeito cibercriminoso, pois eles detêm a informação do *internet protocol* (IP), número de identificação de cada dispositivo conectado à Rede (Domingos; Roder, 2017, p.63).

Outrossim, em que pese exista forma de identificar o criminoso digital por meio do referido de IP, os mais habilidosos dentre eles se utilizam de ferramentas chamadas *proxys*, que servem para mascarar a localização do agente delinquente em até mesmo três pontos diferentes ao redor do globo, assim, utilizando máquinas com endereços intermediários entre o usuário e o destino a ser alcançado. Dentre essas ferramentas está o TOR (The Onio Router), simples recurso disponível ao público, comum.

Para melhor ilustrar, exemplifica-se por meio do caso real conforme bem destaca GOODMAN (2015, p.16) ao citar o assalto realizado por Vladmir Levin, o qual estava em seu apartamento em São Petersburgo, na Rússia, e subtraiu US$ 10,7 milhões de uma agência do Citibank na Times Square em Nova York, Estados Unidos. A ação contou com o auxílio de cúmplices ao redor do mundo e transferiu grandes somas de dinheiro para diferentes contas bancárias na Finlândia, nos Estados Unidos, Holanda, Alemanha e em Israel. Frente a situação, quem teria jurisdição para o caso? A polícia da Nova York onde a *res furtivae* estava ou as autoridades russas? Ou ainda,

as polícias dos diferentes países para onde a soma foram enviadas? O autor do fato nunca precisou ingressar fisicamente dentro do local para executar o crime e nem precisou transportar a grande quantia de notas de papel, não foi utilizado arsenal bélico e nem máscaras também.

Dessa forma, demonstrando-se que a Internet torna o mundo sem fronteiras, no qual a vítima do delito informático pode estar em território nacional diverso daquele em que o delinquente estava endereçado ao tempo do cometimento do crime, se tornando um verdadeiro problema para delimitar a competência de persecução e julgamento penal.

O ciberespaço de fato não é propriamente um espaço físico, então não pode ser caracterizado como um território, muito menos pertencente a um determinado Estado-nação (Goodman, 2015, p. 16). Da mesma forma, é errônea afirmar que os delitos que ocorrem na Rede sejam tratados como crimes virtuais, haja vista que não são de práticas irreais, trazendo efeitos às pessoas, tanto em caráter patrimonial como psicológico (Costa, 2011, p.33).

Contudo, conforme já estudado, pode-se caracterizar o ciberespaço pelo grande fluxo dados na web por meio das redes de comunicação, fazendo com que ganhe importância a localização da informação, haja vista que ela indicada, mesmo que de forma mínima, o território da ação criminosa (Crespo, 2011, p.117), podendo-se atribuir competência penal sobre determinado fato, porém mais uma vez se enfrenta a problemática, pois como no caso prática, muitas ações podem partir um Estado diverso daquele que atinge o bem jurídico, podendo causar tanto conflitos positivos quanto negativos de jurisdição.

4. A CONVENÇÃO DE BUDAPESTE E A HARMONIZAÇÃO INTERNACIONAL DE LEGISLAÇÕES CONTRA OS DELITOS INFORMÁTICOS

Determinar o correto lugar físico de onde partira determinada ação criminosa, qual foram os caminhos e etapas até que atingir a vítima, conhecido como o *iter criminis*, assim como, onde se encontrava o bem jurídico violado, e o resultado pretendido, demonstra-se que a localização física da prática do ato de um delito

informático por certo possui relevância ao Poder Judiciário, para determinar a competência jurídica, tanto para a persecução quanto para o processo criminal.

Em termos processuais, destaca-se a imprescindibilidade de prova válida a fim de não originar nulidades no processo criminal, diante disso, para determinada autoridade brasileira obtenha dados a respeito de usuários que utilizaram como meio um serviço de rede informática disponibilizada no exterior, ou então, sujeito estrangeiro que voltou a sua ação ao Brasil, o instituto mais usual é a morosa (Jesus; Milagre, 2016, p. 194).

Outrossim, deve-se apontar a possibilidade de utilização de acordos de cooperação internacional por meio do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), do Ministério da Justiça (Wendt; Jorge). Contudo, cumpre destacar que, trata-se de procedimento notoriamente lento, haja vista depender de uma série de requisitos variáveis, uma vez que para cada país que o pedido for feito, deverá ser de acordo com os requisitos normatizados em suas legislações, não havendo uma padronização de larga escala relacionadas aos pedidos.

O procedimento relacionado às cooperações, já se mostrava ser de fato bastante lento, em alguns casos inofensivos, frente a volatilidade das provas digitais extremamente necessárias quando se trata de crimes que perpetrados por meio da Rede, assim como contra bens que não muitas vezes não se encontram em espaços físicos para que seja feito exames periciais nos moldes tradicionais dos códigos de processos penais (Domingos; Roder, 2017, p. 65).

Ademais, além do processamento vagaroso, essa cooperação internacional apenas se faz possível devido ao Brasil ser signatário de *Mutual Legal Assisitance Treaties* (MLATs) – Acordos de Assistência Mútua em Matéria Penal – que são as determinações que possibilitam essa troca mútua de dados, provas, informações e diligências necessárias em processos criminais, inclusive, é o método a ser utilizado quando se trata de delitos informáticos (Jesus; Milagre, 2016, p. 195.).

Atualmente, o Brasil possui acordos bilaterais de *Mutual Legal Assisitance Treaties* com 20 países (Brasil, 1994), que podem ser utilizados para requisições de provas a fim de embasar investigações policiais e processos judiciais relacionados

com os delitos informáticos, sendo o um dos mais recentes datado do ano 2017, homologando meio do Decreto nº 9.130 de 2017 com a Bélgica (Brasil, 2017). Outrossim, os acordos possuem alcance com Estados da Europa, Ásia e Américas.

Por meio de todos esses atos normativos deferindo o aceite de cooperar, mostra-se que o Brasil possui ferramentas e meios de comunicação com outros Estados a fim de obter provas e investigar delitos, contudo conforme demonstrado, são métodos lentos e ineficazes, a depender da ação criminosa e do conhecimento técnico do autor (Jesus; Milagre, 2016, p. 195).

Ante o exposto, por certo há a necessidade de institutos legais imbuídos de eficácia investigativa e processual com a intenção de conter a prática delitiva no ciberespaço, uma vez que uma das finalidades do Direito Penal se trata justamente de positivar atos que quando praticados sejam criminalmente punidos, não havendo regramento, ou quando haver, de alguma forma for impedido de correta aplicação, demonstrará ao possível criminoso digital forte possibilidade de sair impune.

Dessa forma, preocupado com a problemática dos delitos informáticos desde o ano de 1996, o Comitê Europeu de Crimes e Problemas, *The European Committee on Crime Problems*, decidiu mediante a resolução de Novembro de 1996, estabelecer um comitê de especialistas para tratar de aspectos relacionados aos crimes cibernéticos. Posteriormente, em 04 de fevereiro de 1997, uma comissão de ministros munidos de relatórios e recomendações dos especialistas em delitos informáticos e processualistas penais, estabeleceu-se novo comitê de especialistas em ciberespaço (Martín, 2012, p. 1670-1674.).

O denominado Comitê de Especialistas em Ciberespaço iniciou as suas atividades em abril de 1997, sendo encarregados encomendar um projeto de convenção sobre cibercriminalidade até 31 de dezembro de 2001. Após celebração de uma dezena de sessões, reuniões e encontros complementares, fora apresentada aos Ministros que haviam feito a requisição o projeto de lei, após a versão final ter sido revisada, fora submetida ao Comitê de Especialistas em Ciberespaço durante a 50ª sessão do plenário em junho de 2001, posteriormente, fora enviada ao Comitê de Ministros para adoção para após ser remetida aos países membros para firmarem o pacto (Martín, p. 1667-1685).

Nesse sentido, em 21 de setembro de 2001 no âmbito do Conselho da Europa, fora elaborada e posteriormente firmada por mais de 40 países, como Estados Unidos, Canadá, África do Sul e Japão, a Convenção sobre a Cibercriminalidade (Martín, p. 1667), comumente conhecida como a Convenção de Budapeste (Budapeste, 2001), a qual entrou em vigor, em 01 de julho de 2004 (Cidrão; Muniz; Alves, 2018, p. 66-82), postulando a positivação de uma política criminal de alcance multinacional a fim de fornecer proteção aos indivíduos presentes na sociedade informacional contra as ações e o sujeitos delinquentes presentes no ciberespaço, (Cidrão; Muniz; Alves, 2018, p. 66-82).

A Convenção de Budapeste se trata do mais amplo e evoluído instrumento jurídico de cooperação internacional na matéria de delitos informáticos, buscando formas de conter os delitos informáticos, observando de forma especificada a segurança das redes computacionais, das violações de direitos autorais, fraudes cometidas utilizando-se de computadores e pornografia infantil. Para o Conselho da Europa, havia ciência da potencialidade dos crimes cometidos por meio da Rede, convencidos na necessidade de buscar, como medida de prioridade, uma política criminal comum de proteção da sociedade contra essa crescente prática criminosa, buscou-se então, consonância jurídica entre as soberanias dos estados membros, concebendo a caracterização do ciberespaço como um espaço comum que é usufruído por todos os cidadãos que possuem acesso e trafegam na web (Cidrão; Muniz; Alves, 2018, p. 66-82).

Nesse sentido, os relatores ao elaborarem o texto da Convenção de Budapeste, debateram aspectos não apenas importante em relação a competência, mas também sobre questões de direito material e processual, assim, o documento não fora concebido apenas com a intenção de novos tipos penalizáveis, mas também para fomentou a criação de procedimentos processuais penais de direito penal internacional, por meio de acordos referentes à tecnologia da informação (Cidrão; Muniz; Alves, 2018, p. 78).

Ademais, por essa perspectiva, faz-se necessário destacar os objetivos da referida Convenção, assim, conforme destaca a doutrina de VELASCO SAN MARTÍN (2012, p. 1692), primeiramente se destaca a intenção de harmonização das

disposições legais relacionadas à cibercriminalidade; oferecer aos países membros faculdades necessárias sobre o procedimento interno para persecução investigativa de delitos informáticos e outras atividades contra os sistemas informacionais, para que haja obtenção de provas contidas em dispositivos e sistemas em Rede – é importante destacar que a Convenção de Budapeste traz de roteiro que não necessariamente exige-se adoção por parte do Estado membro, entretanto, que sejam utilizadas definições equivalentes, para unificar os conceitos trazidos e viabilizar determinados procedimentos (Cidrão; Muniz; Alves, p. 78.). Ainda, destaca-se como um dos objetivos principais da Convenção de Cibercriminalidade, o regime ágil e efetiva de cooperação internacional entre os países membros (Martín, 2012, p. 1695).

Nesse sentido, conforme aponta o trabalho, uma das maiores problemáticas relacionadas aos crimes digitais se refere a jurisdição aplicável ao fato, situação extensivamente discutida no âmbito do Conselho da Europa. Os peritos do Comitê sobre o Ciberespaço debateram e propuseram hipóteses para que as autoridades judiciais tivessem a capacidade efetiva de abordar os aspectos da jurisdição criminal. Na perspectiva, ao final dos debates, o referido Comitê redator decidiu por incluir princípios norteadores para definição do local da prática dos crimes, propondo solução para o problema de aplicação da legislação no ciberespaço, inclusive aspectos para solucionar problemas de bis in idem, quando dois ou mais países estão envolvidos nos crimes, assim como a resolução de conflitos positivos e na prevenção de conflitos negativos de jurisdição (Martín, 2012, p. 1727-1732).

Dessa forma, a Convenção sobre Cibercriminalidade disponibilizou no texto do seu Art. 22 determinações legais a serem observadas a fim da correta aplicação da competência julgadores. Primeiramente, o dispositivo define no item nº 1 (Budapeste, 2001), positiva que cada parte adotará as medidas legais que se revelarem necessárias para estabelecerem competência sobre qualquer uma das tipificações contidas do artigo 2º ou artigo 11º da referida Convenção quando se tratar de ato cometido: a) no seu território, nesse ponto observa-se a adoção do princípio da territorialidade adotado pelo redator; b) a bordo de um navio ou aeronave do Estado, a bordo de aeronave matriculada sob as leis do país ou; c) tiver sido praticada por algum dos cidadãos nacionais se a infração for punível criminalmente onde a ação

tenha sido cometida, em relação ao ponto a e b, a doutrina destaca que se trata de uma variante do princípio da territorialidade ou então; d) não for de competência territorial de nenhum dos Estados (Martín, p. 1777-1782).

De outro canto, ainda em relação ao item nº 1 do artigo 22 da Convenção, o item nº 2 estipula que cada parte poderá se reservar ao direito de não aplicar, ou então, aplicar apenas em casos e condições que sejam específicas as regras de competências previamente estabelecidas no item nº 1 alíneas a e b. Em relação ao Item nº 3, postula-se que o Estado adotará as necessárias medidas que levem a estabelecer a sua competência em relação às infrações contidas no Art. 24, item nº 1 (Conselho da Europa, 2001) do Tratado, quando a autoria do delitos for presumível e se encontre sob o seu domínio territorial e não ser extraditável, após pedido, ao outro país, apenas embasado em sua nacionalidade. De forma suscinta, o item nº 4 informa que a Convenção não excluirá qualquer competência penal que seja exercida por um dos Estados membros em consonância com o seu ordenamento jurídico interno, ou seja, trata-se de confirmar a soberania estatal do país membro.

Outrossim, o item nº 5 do Art. 22 da Convenção de Budapeste, traz dispositivo se mostra deveras interessante ao objetivo do presente estudo, nos seguintes moldes: "...Quando mais que uma Parte reivindique a competência [...], as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal".

Ante o exposto, o redator da referida Convenção, demonstra a necessária preocupação com referente a competência nos delitos informáticos, dada a característica transfronteiriça do ato criminoso, assim, quando mais de um Estado signatário reivindicar competência sobre a suposta ação delinquente prevista no Tratado as partes irão se consultar a fim de determinar a jurisdição mais apropriada para o procedimento penal.

Ainda em matéria de cooperação internacional entre Estados membros, a convenção sobre cibercriminalidade traz rol de princípios aplicáveis, dentre eles, faz-se necessário destacar os Princípio gerais relativos ao auxílio mútuo (Conselho da Europa, 2001), presente no artigo 25 do Pacto. Nesse sentido, postula que os Estados envolvidos concederão entre si auxílio mútuo da forma mais ampla que puderem agir

no que se refere as investigações ou procedimento relativos aos delitos cometidos com ou contra sistemas de dados informáticos. Outrossim, no item nº 2, expõem-se que cada parte irá adotar de forma igualitária medidas legislativas, dentre outras que se revelarem necessárias cumprirem com às obrigações estabelecidas nos artigos 27 e 35 (Conselho da Europa, 2001) da Convenção. Outrossim, destaca-se que o Tratado ainda trouxe na norma, dispositivo para ser utilizado como referência a fim de criar rede de contato investigativa interconectada entre os países membros 24 horas por dia e 07 dias por semana, com o intuito de assegurar a mútua assistência.

Em continuidade ao texto do Art. 25 da Convenção, o item nº 3 expõem que, em casos de urgência, o Estado pode formular pedido de auxílio ou de comunicação através de meios rápidos de comunicação, desde que esses meios de comunicação ofereçam condições necessárias de autenticação e segurança, com a posterior confirmação oficial que o Estado requerido exigir, o qual poderá responder utilizando qualquer um dos meios de comunicação. Por meio do item nº 4, observa-se que os pedidos de auxílio deverão obedecer a condições fixadas no direito interno no país requerido, ou então, pelos tratados de auxílio mútuo, inclui-se os fundamentos que a Estado requerido poderá recusar a cooperar.

Diante disso, destaca-se que a Convenção de Budapeste de 2001, trata-se de completa legislação norteadora de regulamentações legais a respeito dos delitos informáticos, tanto para tipificações quanto acordos mútuos de cooperação, forma de tutelar diplomacia legal entre Estados a fim de encontrar solução sobre qual possui maior interesse processual na conduta criminosa. Ademais, ainda traz a possibilidade de conversação entre nações a fim de aplicação de medidas provisórias para conservação de dados probatórios necessários na investigação (Conselho da Europa, 2001).

Conduto, existem críticas feitas ao Tratado, haja vis que a Convenção trata os países membros de forma idêntica, sem considerar as diferenças tecnológicas, políticas, sociais e econômicas de cada país (Cidrão; Muniz; Alves, 2018, p. 78).

De outro lado, alguns países latino-americanos já ratificaram a Convenção de Budapeste, dentre esses, a Argentina que em 2010, durante a Conferência

Octopus ocorrida entre os dias 23 e 25 de março do referido ano, onde expressará formalmente seu compromisso com o Tratado (Martín, 2012, p. 1708).

Em relação ao Brasil, o Comitê de Ministros do Conselho da Europa no ano de 2019 o convidou a integrar o rol de países que ratificam a Convenção de Budapeste, época em que o governo brasileiro havia manifestado intenção em aderir o Tratado internacional, figurando como observador sem ter direito a voto.

Atualmente, é importante dizer que o Brasil já é signatário da Convenção sobre Cibercriminalidade, ratificado com o decreto nº 11.491, de 12 de abril de 2023 e promovendo e estimulando mudanças importantes na legislação brasileira.

Porém, antes mesmo de ser ratificada, é possível identificar influências da Convenção de Budapeste na legislação interna brasileira, as quais foram inicialmente com a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann. Essa Lei tipifica crimes como invasão de dispositivos informáticos, clonagem de cartões de crédito e difusão de vírus, alinhando-se às categorias de crimes previstas na convenção.

Logo mais o Marco Civil da Internet (Lei nº 12.965/2014) foi uma das primeiras respostas legislativas do Brasil à necessidade de regular a internet de forma abrangente. Embora focado na proteção dos direitos dos usuários e na neutralidade da rede, o Marco Civil também estabelece diretrizes sobre a cooperação internacional em investigações e a preservação de registros de acesso, refletindo princípios da Convenção de Budapeste.

Posteriormente, foi promulgada a Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, estabelece diretrizes para a coleta, armazenamento, uso e compartilhamento de dados pessoais no Brasil. Seu objetivo é garantir a privacidade e a proteção dos dados dos cidadãos, conferindo direitos aos titulares, como o acesso, correção e exclusão de informações. A LGPD também impõe obrigações às empresas e organizações, promovendo a transparência e a responsabilidade no tratamento de dados. A sua vigência fortalece a segurança jurídica e a proteção da privacidade em meio ao crescente uso de tecnologias digitais. Enfim, diversos artigos do Código Penal Brasileiro foram adaptados para incluir crimes cibernéticos. A Convenção de Budapeste influenciou a inclusão de dispositivos que tratam de crimes como a falsificação de documentos digitais e fraudes eletrônicas.

A Convenção de Budapeste enfatiza a cooperação internacional para o combate ao cibercrime, e o Brasil tem trabalhado para fortalecer essa cooperação, especialmente com países que são signatários da convenção. Isso inclui o compartilhamento de provas digitais e a assistência em investigações que envolvem múltiplas jurisdições também tem sido uma referência constante em debates legislativos e propostas no Congresso Nacional. Temas como a proteção de dados, a necessidade de um órgão central de cibercrime e a adaptação das leis penais à realidade digital têm sido discutidos à luz das diretrizes dessa convenção. Apesar do Tratado influenciar em algumas alterações na legislação brasileira, após o Brasil ratificar a Convenção de Budapeste não houve qualquer mudança quanto a temática relacionada à jurisdição criminal, o que demandará forte incentivo estatal e pressão social por meio das instituições para modernização dos instrumentos internos de cooperação jurisdicional, efetivamente influenciando questões de competência do Estado.

5. CONCLUSÃO

Por meio do presente trabalho, fora demonstrada a importância e a necessidade de uma legislação uníssona a nível internacional, a fim de pacificar as jurisdições e tipificações referentes aos delitos informáticos, uma vez que apenas Mutual Legal Assistance Treaties se mostram vagarosos, por vezes ineficazes, dada a complexidade de seus requisitos e lentidão de processamento.

Destarte, a Convenção de Budapeste surgirá no âmbito do Conselho da Europa, justamente com o desafio de homogeneizar as normas entre diferentes Estados para eficaz combate e repressão das práticas criminosas, que além de possibilizar a cooperação internacional na angariação de provas e manutenção de dados voláteis e de necessário arquivamento para a solução dos casos, traz a possibilidade de dirimir os conflitos de competência envolvendo diferentes países que tiveram de alguma forma a ver com o delitos informático, solucionando um importante problema enfrentado pelas autoridades competentes para julgá-los.

Nesse sentido, mostrou-se imperiosa a ratificação do Brasil à referida Convenção de Budapeste, a fim de se tornar parte de um rol internacional de países que adotaram o pacto para igualar as normas internas com a intenção de viabilizar trâmites legais investigativos e processuais referentes ao delitos informáticos, assim como dirimir questões voltadas a jurisdição criminal, evitando conflitos positivos e negativos de competência, inclusive, viabilizando a conversação entre nações para avaliar qual delas possui maior interesse em determinada ação criminosa cuja a prática e resultado tenha passado por diferentes territórios. após o Brasil ratificar a Convenção de Budapeste e ser participante com os demais países não houve qualquer alteração formal ou processual na legislação brasileira, o que nos traz um alerta, sendo necessária a cobrança das instituições para adequação e segurança à sociedade de maneira mais efetiva.

REFERÊNCIAS

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016. Disponível em: https://pt.scribd.com/read/405795372/Manual-de-Investigacao-Cibernetica-A-luz-do-Marco-Civil-da-Internet#. Acesso em: 17 agosto. 2024.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023.** Convenção sobre o Crime Cibernético. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 17 agosto. 2024.

BRASIL. **Decreto nº 9.130, de 17 de agosto de 2017**. Promulga o Tratado entre a República Federativa do Brasil e o Reino da Bélgica sobre Auxílio Jurídico Mútuo em Matéria Penal, firmado em Brasília, em 7 de maio de 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9130.htm. Acesso em: 17 agosto. 2024.

BRASIL. **Decreto-Lei nº 3.689, de 03 de outubro de 1941**. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 17 agosto. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Lei Carolina Dieckmann. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 agosto. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 agosto. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 agosto. 2024.

BRASIL. Ministério Público Federal. **Tratados de Auxílio Jurídico Mútuo em Matéria Penal**. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/tratados/tratados-de-mutual-legal-assistance-auxilio-juridico-mutuo-em-materia-penal. Acesso em: 17 agosto. 2024.

CIDRÃO, Tais Vasconcelos; MUNIZ, Antônio Walber; ALVES, Ana Abigail Costa Vasconcelos. A Oportunidade e Necessária Aplicação do Direito Internacional nos Ciberespaços: Da Convenção de Budapeste à Legislação brasileira. **Brazilian Journal of International Relations**, Marília, v. 7, ed. 1, p. 66-82, jan./abr. 2018.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23.XI.2001. Disponível: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 17 agosto. 2024.

COSTA, Marcelo Antonio Sampaio Lemos. **A Análise Forense no Contexto da Resposta a Incidentes Computacionais**. 3. ed. Campinas: Millennium Editora, 2011.

COUNCIL OF EUROPE. **Convention of Cybercrime de 23 de novembro de 2001**. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Acesso em: 17 agosto. 2024.

CRESPO, Marcelo Xavier de Freitas. **Crimes Informáticos**. São Paulo: Saraiva, 2011.

DOMINGOS, Fernanda Teixeira Souza; RODER, Priscila Costa Shreiner. Obtenção de provas digitais e jurisdição na Internet. **Caderno de Estudos**: Investigação e prova nos crimes cibernéticos, São Paulo, p. 55-84, 2017. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 17 agosto. 2024.

GIBSON, William. **Neuromancer**. Fábio Fernandes (Trad.). 5. ed. São Paulo: Aleph, 2016.

GOODMAN, Marc. **Future Crimes**: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. Gerson Yamagami (Trad.). São Paulo: HSM Editora, 2015.

GUARAGNI, Fábio André; RIOS, Rodrigo Sánchez. Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea. **Revista de Estudos Criminais**, Porto Alegre, v. 18, n. 73, p. 167-196., abr./jun. 2019. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=151418. Acesso em: 30 mar. 2020. Acesso em: 17 agosto. 2024.

HUNGRIA, Nélson. **Comentários ao Código Penal**: art. 11 a 27. v. 1, 4. ed. t. II. Rio de Janeiro: Forense, 1958.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

LÉVY, Pierre. **Cibercultura**. Carlos Irineu da Costa (Trad.). São Paulo: Editora 34, 1999.

PINHEIRO, Patrícia Peck Garrido. **Direito digital**. 5. ed. São Paulo: Saraiva, 2014.

PORTAL DA PRIVACIDADE. **Brasil pode aderir à Convenção de Budapeste sobre crimes cibernéticos**. [*S. l.*]: PortalDaPrivacidade, 2021. Disponível em: https://www.portaldaprivacidade.com.br/brasil-pode-aderir-a-convencao-de-budapeste-sobre-crimes-ciberneticos/. Acesso em: 17 agosto. 2024.

SAN MARTÍN, Cristos Velasco. **La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet**. Spanish Edition: Tirant lo Blanch. Edição do Kindle, 2012.

SHIMABUKURO, Adriana. Cibercrime: quando a tecnologia é aliada da lei. **Caderno de Estudos**: Investigação e prova nos crimes cibernéticos, São Paulo, p. 17-32, 2017. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 17 agosto. 2024.

TORPROJECT. **Homepage**. Disponível em: https://www.torproject.org/. [*S. l.*], [*S. d.*]. Acesso em: 04 mai. 2021.

VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Editora Fórum, 2013. Disponível em: https://www.academia.edu/31426233/CRIMES_INFORM%C3%81TICOS_-_Conforme_a_Lei_no_12.737_2F?auto=download. Acesso em: 17 agosto. 2024.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. 2. ed. Rio de Janeiro: Brasport, 2013. Disponível em: https://pt.scribd.com/read/436286025/Crimes-Ciberneticos-ameacas-e-procedimentos-de-investigacao#. Acesso em: 17 agosto. 2024.