1 Introdução

A partir do debate sobre as novas tecnologias e sobre a necessidade de regulação das ações que envolvem essas questões, o presente artigo tem por objetivo discutir o panorama global e brasileiro dos crimes cibernéticos à luz da Convenção de Budapeste.

Ressalte-se que a carência de produção acadêmica brasileira sobre aspectos relacionados aos crimes cibernéticos justifica a importância do tema proposto.

Assim, a partir de pesquisa bibliográfica e documental, e observando a aceleração de esforços para pactuação de regulação dessas questões, o artigo busca problematizar o tema dos delitos virtuais os quais fornecem relevantes assuntos para o debate brasileiro: se há a necessidade de ratificação do Brasil à Convenção de Budapeste.

Ao final decorre disso a discussão deste artigo acerca de como a ratificação da citada Convenção pelo Estado brasileiro poderia contribuir e se são necessárias para a regulação dos crimes cibernéticos no Brasil.

2 Da Sociedade da Informação para a Sociedade Digital: as Novas Tecnologias

Para se analisar o tema proposto neste trabalho sobre o panorama dos crimes cibernéticos à luz da Convenção de Budapeste e sobre o debate brasileiro acerca da necessidade de ratificação do Brasil à Convenção torna-se relevante sublinhar algumas linhas acerca das novas tecnologias e sobre a passagem da sociedade da informação para a sociedade digital.

Inicialmente, cumpre destacar que, a partir de um ponto de vista histórico, as organizações sociais das pessoas começaram com as atividades agrícolas. Daí as sociedades foram se transformando e se adequando notadamente a revoluções industriais as quais podem-se subdividir até o momento em quatro revoluções.

Enquanto a primeira revolução industrial utilizou a água e as máquinas a vapor para a mecanização da produção, a segunda revolução transformou a energia elétrica e a eletricidade para o processo de produção.

Em seguida, a terceira revolução industrial se apoderou do desenvolvimento da eletrônica e do conhecimento e da tecnologia da informação, no contexto da sociedade da informação, e iniciou um caminho de automação industrial ligada às redes mundiais de computadores.

Por fim, a chamada quarta revolução industrial, ou a revolução 4.0, nesta época contemporânea, segundo entendimento de Schawab (2016), dispõe de dados, a chamada nova moeda digital, para impulsionar o processo automatizado de produção. Teve sua origem na Alemanha, em 2010, impulsionada por projetos de estratégias de alta tecnologia com a finalidade de digitalização e avanço da produção industrial alemã.

Em verdade, constata-se que as novas tecnologias de dados estão abrangendo todas as áreas da vida humana e se integrando ao nosso cotidiano em uma velocidade exponencial, potencializada pelos efeitos da pandemia do COVID-19 em nível global, desde a robótica, a inteligência artificial AI, a integração da internet das coisas e a biotecnologia.

Dessa feita, essas novas tecnologias compõem um conjunto de tecnologias disruptivas como a inteligência artificial, a robótica, o *big data*, a nanotecnologia, a internet das coisas, computação em nuvem, *blockchain*, a impressão 3D, do computador quântico, do algoritmo, entre tantas outras.

Não se pode olvidar que essas transformações sociais e empresariais estão repercutindo seus efeitos nas relações sociais e no direito (SANTOS, 2021).

Por fim, impende observar que a chamada quarta revolução industrial não se utiliza de cada tecnologia de forma isolada. Não. Ela se conecta, interligando os mundos físicos e digitais, em um sistema de redes, desde a vida cotidiana humana no planeta Terra, até os sistemas de produção de manufatura avançada, em uma cadeia produtiva absolutamente interligada que está transformando o mundo dos negócios e as inovações.

Pelas razões expostas denota-se a importância desta parte inicial sobre as novas novas tecnologias e sobre a passagem da sociedade da informação para a sociedade digital para o desenvolvimento do tema proposto acerca do panorama dos crimes cibernéticos à luz da Convenção de Budapeste e sobre o debate brasileiro acerca da necessidade de ratificação do Brasil à Convenção. É o que será visto a seguir.

3 O panorama dos crimes cibernéticos à luz da Convenção de Budapeste

Após a breve abordagem sobre as novas tecnologias e sobre a transformação da sociedade da informação para a sociedade digital passa-se ao estudo do panorama dos crimes cibernéticos à luz da Convenção de Budapeste.

3.1 A Convenção de Budapeste e os crimes cibernéticos

No intuito de se estudar a Convenção de Budapeste mister ressaltar algumas linhas sobre o direito internacional público.

No que se refere ao direito internacional público ou o direito das gentes, suas origens históricas surgiram na Antiguidade. Contudo, a partir de um corte epistemológico, segundo Hildebrando Accioly (2010), o direito internacional passa a ser objeto da ciência jurídica com os Tratados de Munster e Osnabruck, atualmente duas cidades alemãs, também chamados de Paz de Vestfália, que puseram fim à Guerra dos Oitenta Anos, assinados em 30 de janeiro de 1648.

Nesse período histórico, cumpre destacar o holandês Hugo de Groot, considerado um dos fundadores do direito internacional a partir do direito natural.

Os documentos internacionais decorrentes da Paz de Vestfália inauguraram uma noção inicial de paz, fundamentada no equilíbrio do poder para soluções de controvérsias entre Estados, cuja ideia de paz foi aprofundada no Congresso de Viena, em 1815, e no Tratado de Versailles, em 1919, que encerrou oficialmente a 1ª Grande Guerra e criou a Liga das Nações.

Pois bem. No ambiente da Liga das Nações surgiu, em 1921, o Tribunal Permanente de Justiça Internacional ou a Corte Permanente de Justiça Internacional. A sede do Tribunal até os dias atuais está instalada no Palácio da Paz, em Den Haag, nos Países Baixos. Em 1946, naquele momento sob a égide da ONU, passou a ser chamado de Tribunal Internacional de Justiça.

Já no contexto do final da 2ª Grande Guerra, aparece no cenário mundial sinais de uma nova era, com a Declaração Universal de Direitos Humanos, com seus Pactos subsequentes e a criação das Organizações das Nações Unidas (ONU). A noção de direitos humanos como resposta às atrocidades da Segunda Guerra inaugurou uma nova

perspectiva internacional, especialmente com a inserção da pessoa humana como sujeito de direitos (LIMA, 1974).

Cumpre examinar também, ainda no contexto da necessidade do estabelecimento de paz entre os Estados, que surgiram normas internacionais, especialmente fundamentadas na soberania dos Estados, que as firmam e as criam como reflexos de sua soberania.

Assinale-se ainda que as fontes do direito internacional podem ser arroladas notadamente como os costumes, os princípios gerais de direito, as decisões judiciais e as Convenções e os Instrumentos internacionais.

Nesse quadro, importante papel teve a Convenção de Viena, firmada em 1969. Tratava-se de fonte de direito internacional que codificou as regras consuetudinárias e foi em seguida reforçada pela Convenção de 1986. Demais disso, definiu convenções como acordos regidos pelo direito internacional, como acordo de vontades entre dois sujeitos de direito internacional.

Nessa seara, a Convenção de Budapeste ou a Convenção sobre o Cibercrime, adotada pelo Comitê de Ministros do Conselho da Europa e pelos Estados Unidos, Canadá, Japão e África do Sul, na Sessão 109 de 08 de novembro de 2001, foi aberta à assinatura em Budapeste, em 23 de Novembro de 2001, e entrou em vigência em 01 de julho de 2004. Constitui-se em um tratado internacional sobre direito penal e direito processual penal, para promover a cooperação entre os Estados no combate aos crimes praticados por meio de Internet e com uso de computadores.

Não se pode perder de vista que essa Convenção decorreu do novo panorama global, instaurado a partir da terceira revolução industrial, a chamada sociedade da informação, a qual iniciou um caminho de automação industrial ligada às redes mundiais de computadores.

Convém ressaltar que esse novo panorama global fez surgir delitos transnacionais os quais ultrapassam os limites territoriais dos Estados soberanos, com novas características em referência a bens jurídicos imateriais e difusos.

Para enfrentar esses novos desafios mundiais, tanto a academia quanto o ambiente militar, esforçaram-se para o desenvolvimento dessa matéria. Até que, com o cair das Torres Gêmeas, nos Estados Unidos, em 2001, esses esforços foram intensificados e culminou com a Convenção sobre o Cibercrime.

Em 2003, o Protocolo Adicional à Convenção de Budapeste tratou da criminalização de atos de natureza racista e xenofóbica cometidos por meio de sistemas de computador, firmado em Estrasburgo em 28 de janeiro de 2003, com vigência a partir de maio de 2006.

Além disso, há um Segundo Protocolo sobre evidências eletrônicas, com 25 artigos, entre eles sobre ferramentas tecnológicas, formas de cooperação direta entre países e empresas provedoras de serviços estrangeiras, para informações sobre registros de nomes de domínio e informações de clientes, e entre autoridades de países distintos, para revelação acelerada de dados informáticos em situações de emergência, bem como assistência jurídica mútua emergencial, vídeo conferências e investigações conjuntas. Há também itens sobre as condições e salvaguardas para a proteção de dados pessoais, além de disposições sobre eficácia, vigência e aplicabilidade da norma no plano internacional, com adoção prevista para novembro de 2021.

Por fim, importa salientar que apesar de a Convenção de Budapeste ter sido atualizada a Diretiva 2013/40/UE (2013) do Parlamento Europeu manteve o seu texto original como base.

Especificamente sobre os crimes cibernéticos, é interessante frisar que a Convenção referida apenas recomenda a tipificação de delitos, sem vinculação coercitiva, mas, por outro lado, serve de parâmetros aos Estados para uma almejada uniformização legislativa sobre esse tema.

De início, com esse objetivo de uniformização da matéria, a Convenção de Budapeste traça algumas definições importantes, entre elas, sistema de computador, dados de computador, provedor de serviços e tráfego de dados:

> *Article 1 – Definitions*
>
> *For the purposes of this Convention:*
>
> *a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;*
>
> *b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;*

> *c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.*
>
> *d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying servisse* (2001).

Além desse ponto, vale lembrar que a Convenção de Budapeste aborda tanto aspectos materiais quanto processuais penais, contudo, para fins deste artigo, restringir-se-ão aos aspectos materiais penais especialmente no que tange aos crimes cibernéticos.

Pois bem. Nos termos da Convenção, no Capítulo II, sobre medidas a serem tomadas em nível nacional sobre direito material criminal, constam as seguintes diretrizes para tipificação no Título 1, como ofensas contra a confidencialidade, integridade e disponibilidade de dados de computadores e sistemas notadamente: acesso ilegal, interceptação ilegal, interferência de dados, sistemas de interferência, mau uso de equipamentos; no Título 2, sobre ofensas relacionadas a computadores, entre elas falsificações e fraudes relativas a computadores.

Não se pode esquecer ainda do que consta nos Títulos seguintes da Convenção de Budapeste, sobre ofensas de conteúdo como pornografia infantil e ofensas relacionadas a direitos autorais e relacionados.

Já o Protocolo Adicional à Convenção de Budapeste, de 2003, que tratou da criminalização de atos de natureza racista e xenofóbica cometidos por meio de sistemas de computador traz definições relevantes para o tema tais como material racista e xenofóbico, bem como estabelece que a interpretação do Protocolo deverá ser feita da mesma forma que da Convenção.

> *Article 2 – Definition*
>
> *1 For the purposes of this Protocol: "racist and xenophobic material" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race,*

> *colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.*
>
> *2 The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention* (2001).

Impende observar que constam nas diretrizes para tipificação a disseminação de material racista e xenofóbico por meio de computadores; ameaças e insultos racistas e xenofóbicos e negação, minimização total, aprovação ou justificativa de genocídio ou crimes contra a humanidade.

Por fim, em virtude dessas considerações é possível apurar que, de forma sintética, a Convenção de Budapeste trata dos crimes cibernéticos subdivididos em quatro categorias:

a) proteção da confiabilidade, integridade e disponibilidade dos sistemas de computador e dizem respeito ao acesso e interceptação ilegais, cujo elemento subjetivo é o dolo, apesar de haver controvérsias, as quais defendem a necessidade da tipificação de condutas sob o manto da culpa, como para a interferência de dados e sistemas e o mau uso de equipamentos;

b) danos relacionados a computador e à verdade das informações cujas condutas estão ligadas à falsificação e à fraude que comprometem a veracidade dos dados inseridos no ambiente das redes;

c) danos relacionados ao conteúdo especialmente sobre pornografia infantil. Trata-se de um termo vago como oferecimento e disponibilidade desse material, em ambiente aberto ou fechado, desde os atos preparatórios, além de estabelecer que as imagens com cenas pornográficas podem designar menores ou os que aparentem menoridade. Tipifica-se assim a conduta de imagens pornográficas de pessoas que já atingiram a maioridade. Significa dizer que imagens de um jovem captadas há muito tempo restariam atípicas se, no presente momento, essa vítima houvesse atingido a maioridade. Dessa forma, a Convenção ampliou o campo de punibilidade penal. Ainda, cabe ressaltar que pornografia infantil difere de pedofilia, que, além de ter abrangência maior, abarca as condutas, notadamente, de estupro envolvendo menores, atentado violento ao pudor, prostituição infantil, drogas, distribuição de material pornográfico;

d) transgressão de direitos autorais e correlatos que se referem a condutas dolosas, lembrando a posição da respeitada doutrina sobre a tipificação de condutas culposas e com escala comercial.

Deflui disso a importância da Convenção de Budapeste uma vez que esse Instrumento internacional desenha condutas praticadas em ambiente de rede, não as fora dele, abarcando, desta forma, nas palavras de Rossini (2004), apenas os fatos típicos ocorridos exclusivamente no Ciberespaço, "podendo receber a denominação de delito telemático dada a peculiaridade de ocorrer no e a partir do inter-relacionamento entre os computadores em rede telemática usados na prática delitiva".

3.2 O panorama do debate brasileiro sobre os crimes cibernéticos e a necessidade de ratificação do Brasil à Convenção de Budapeste

Com a sucinta análise acerca das novas tecnologias e da transformação da sociedade da informação para a sociedade digital, bem como alguns apontamentos sobre a Convenção de Budapeste e os crimes cibernéticos contidos no ambiente do direito material penal, passa-se ao panorama brasileiro e ao debate sobre a necessidade de ratificação do Brasil à Convenção de Budapeste.

Para enfrentar esse debate ainda que de forma não exauriente retorna-se a questões de direito internacional e direito doméstico.

Em apertada síntese, sem adentrar nas teorias monistas, dualistas ou intermediárias, é possível identificar que a relação entre o direito internacional e o direito interno, no Brasil, se dá pela aplicação dos arts. 49, I, e 84, VIII, da Carta brasileira de 1988. O Supremo Tribunal Federal (STF) brasileiro entende que os tratados de direito internacional ingressam no ordenamento interno em forma de lei ordinária.

Outro dispositivo constitucional relevante é a Emenda Constitucional nº 45/04, que alterou o art. 5º, § 3º, da Constituição de 1988, institui que os tratados e convenções internacionais sobre direitos humanos que forem aprovados em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes a emendas constitucionais. para a qual os tratados internacionais serão

incorporados em nível constitucional quando forem aprovados segundo as regras formais das emendas.

Nessa seara, dessume-se que, nos termos do entendimento do STF, a Convenção referida ingressará no ordenamento interno brasileiro em forma de lei ordinária.

No que tange especificamente aos crimes cibernéticos, também conhecidos como crimes informáticos, crimes eletrônicos ou e-crime, *cybercrime*, ou ainda, crimes digitais, segundo adoção do Conselho Nacional de Justiça (CNJ), são conceituados pela doutrina e pela legislação brasileira. Sem a intenção de esgotar o tema, podem-se pinçar alguns conceitos, entre eles, Ferreira (2000, p. 207-237), define crime de informática como "toda a ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão."

Na mesma linha, Rossini (2004, p. 110) denomina delitos informáticos os que alcançam não somente aquelas condutas praticadas em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível conexão à rede mundial de computadores, ou a qualquer outro ambiente telemático. Para o jurista, delito informático é gênero, do qual delito telemático é espécie.

Importante destacar que entre as categorias de delitos em ambiente de rede já assinaladas anteriormente neste trabalho, entre elas a confiabilidade, a integridade e a disponibilidade de dados, que tratam do acesso e interceptação ilegais, para nós, nesses casos, podem-se punir atos preparatórios, como no crime de quadrilha ou bando (art. 288 do Código Penal brasileiro).

A Lei n. 12.737, de 30 de novembro de 2012 (2021), dispõe sobre a tipificação criminal de delitos informáticos e altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940, o Código Penal e especifica a invasão de dispositivo informático:

> Art. 154-A, os crimes cometidos por meios informacionais
>
> Art. 154-A. Invadir disposto informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

O ser humano pratica condutas hodiernamente e, de acordo com o pacto social, despoja-se de parte de sua liberdade em favor da ordem social. Assim, a sociedade na qual está inserido o homem individual escolhe quais condutas devem ser punidas com mais rigor, e assim sucessivamente. Dessa forma, as condutas mais graves serão abarcadas pelo direito penal e, para as condutas intermediárias, podem-se aplicar sanções de natureza civil ou administrativa. Ainda, para a maioria da doutrina, as condutas praticadas por meio da internet geram o seu uso indevido, com a criação de condutas que espelham a necessidade de sua tipificação diante da sociedade de risco.

Nessa linha de entendimento, sob um contexto histórico, Albuquerque (2006) aponta três tipos de reformas legislativas: a) na década de 70, a reforma que enfrentou a privacidade através de legislação específica; b) em meados da década de 80, o desafio recaiu sobre delitos de natureza econômica e patrimonial. Nesse caso, não se estendeu as infrações já existentes, mas houve edição de leis específicas; c) já no final da década de 80, a terceira onda de reforma penal tratou da propriedade intelectual.

Impende observar que, segundo Albuquerque (2006), a legislação brasileira atendeu parcialmente a segunda e terceira ondas de reformas penais cujos fundamentos são a promulgação da Constituição Federal de 1988; a edição da Lei nº 9.507/97, sobre *habeas data*; e a edição da Lei nº 9.983/00, sobre a reforma do Código Penal, e da Lei nº 9.609/98, sobre a proteção da propriedade intelectual de programas de computador e sua comercialização no país.

Oportuno se torna dizer também que são indicados dois métodos de reforma penal: a) a reforma do Código Penal, com a introdução de novos artigos para oferecer proteção contra condutas ilícitas; b) a adoção de legislação específica, com fundamento no processo de descodificação da legislação e na verticalização do direito constitucional, com leis específicas desprendidas do Código Penal.

Sem adentrar nas controvérsias desses dois métodos, podem-se apresentar algumas medidas que estão sendo tomadas pelo Brasil.

Um exemplo é o Projeto de Lei 2.639/20 (2020), a Lei sobre Liberdade, Responsabilidade, Transparência na Internet, ou o PL das Fake News que estabelece

normas relativas à transparência de redes sociais e de serviços de mensagens privadas, sobretudo no tocante à responsabilidade dos provedores pelo combate à desinformação e pelo aumento da transparência na internet, à transparência em relação a conteúdos patrocinados e à atuação do poder público, bem como estabelece sanções para o descumprimento da lei.

Impende lembrar que a Convenção de Budapeste não tratou das *Fake News*, uma vez que em meados de 2001 esse tema ainda não era recorrente no cenário mundial tampouco doméstico.

Há também o Decreto n. 10.222, de 5 de fevereiro de 2020 (2020) que aprova a estratégia Nacional de Segurança Cibernética, o chamado E-Ciber

Segundo dados da Agência Câmara de Notícias (2021), em 2017, mais de 70 milhões de pessoas foram vítimas de crimes cibernéticos no Brasil. No ano seguinte, 89% dos executivos do país foram vítimas de fraudes cibernéticas. O Brasil é o segundo país com maior prejuízo provocado por esse tipo de ataque.

Esses dados fazem parte de um diagnóstico que compõe o decreto sobre a Estratégia Nacional de Segurança Cibernética, Decreto 10.222/20 (2021).

Em verdade, o Brasil foi convidado a aderir à Convenção de Budapeste em 2019 e sua validade tem o prazo de três anos.

Em consonância com informações fornecidas pela Agência Câmara de Notícias (2021), a mensagem de adesão está em análise na comissão, onde tem parecer, pela aprovação, do deputado Rubens Bueno (Cidadania-PR).

Bueno (2021) cita dois principais eixos do acordo internacional:

a) o compromisso, dos Estados Partes, de elaborar leis penais que tipifiquem e punam as condutas descritas no texto;

b) o outro eixo é composto pelas medidas de cooperação internacional. Assim, os Estados Partes devem se comprometer a extraditar e a prestar assistência, mesmo que não haja acordos bilaterais com o outro país, tanto em medidas cautelares quanto em investigações. Um órgão brasileiro deve ser o responsável pela assistência imediata nas investigações ou procedimentos relacionados a crimes de computador, e deverá funcionar em sistema de plantão de 24 horas, sete dias por semana.

Conforme a diretora do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça, Silvia Amélia Fonseca de Oliveira, há

mais um eixo importante na convenção: a possibilidade de capacitação. A diretora afirma que “o ingresso do Brasil no comitê faz com que o Brasil e os agentes públicos brasileiros tenham acesso a essa capacitação, aumentando a nossa capacidade interna de enfrentamento aos delitos e reforçando a cooperação internacional”. E ressalta ela que não se trata apenas da adesão à convenção e às normas dispostas hoje na convenção. "Trata-se também do ingresso do Brasil numa comunidade que passa a discutir os pontos necessários ao enfrentamento da cibercriminalidade, dos crimes cibernéticos” (2021).

Além desses aspectos é interessante frisar que em audiência pública da Comissão de Relações Exteriores e de Defesa Nacional da Câmara, deputados e especialistas defenderam a adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético, celebrada em 2001 (MSC 412/20) (2021).

Ademais, foram tomadas como medida o PDL 255/21, Projeto de Decreto Legislativo de Acordos, tratados ou atos internacionais, que aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001 (2021).

Ainda em consonância com dados da Agência Câmara de Notícias (2021), o chefe da Divisão de Combate ao Crime Transnacional do Ministério das Relações Exteriores, Eric do Val Lacerda Sogocio, também defende que chegou o momento de o Brasil aderir ao acordo.

> No Itamaraty, chegamos à conclusão de que seria o momento adequado de o Brasil aceitar o convite do Conselho da Europa, por algumas razões. Uma delas é que daria instrumentos adicionais para os órgãos de persecução criminal obterem informações e provas em processos criminais. Também, como parte da convenção, o Brasil passaria a receber o reconhecimento de que suas leis e suas políticas de combate ao crime cibernético e de proteção de dados são compatíveis com normas reconhecidas internacionalmente (2021).

No que se refere ao trato da matéria processual penal e da cooperação internacional, ressalta-se a importância dessas medidas para o combate da nova criminalidade transnacional e a necessidade de adoção de procedimentos uniformes contra

os *cybercrime* e contra paraísos informáticos criados pela territorialidade do direito penal interno de cada Estado-membro.

Em virtude dessas considerações é possível defender a ratificação do Brasil à Convenção de Budapeste para possibilitar o alinhamento desse país aos parâmetros internacionais de combate à criminalidade transnacional, com medidas de enfrentamento a este novo cenário mundial, no contexto da quarta revolução industrial, e seus desafios cada vez mais céleres em uma velocidade exponencial jamais vista pela humanidade e ainda potencializada pelos efeitos da pandemia do COVID-19, mas sempre observando os *standarts* internacionais de direitos humanos.

4 Considerações finais

A chamada quarta revolução industrial não se utiliza de cada tecnologia de forma isolada. Não. Ela se conecta, interligando os mundos físicos e digitais, em um sistema de redes, desde a vida cotidiana humana no planeta Terra, até os sistemas de produção de manufatura avançada, em uma cadeia produtiva absolutamente interligada que está transformando o mundo dos negócios e as inovações.

Decorre disso a importância da análise realizada sobre as novas tecnologias e sobre a passagem da sociedade da informação para a sociedade digital para o desenvolvimento do tema proposto acerca do panorama dos crimes cibernéticos à luz da Convenção de Budapeste e sobre o debate brasileiro acerca da necessidade de ratificação do Brasil à Convenção

Ressalte-se que a Convenção de Budapeste, de 2001, constitui-se em um tratado internacional sobre direito penal e direito processual penal, para promover a cooperação entre os Estados no combate aos crimes praticados por meio de Internet e com uso de computadores.

Especificamente sobre os crimes cibernéticos, é possível frisar que a Convenção referida apenas recomenda a tipificação de delitos, sem vinculação coercitiva, mas, por outro lado, serve de parâmetros aos Estados para uma almejada uniformização legislativa sobre esse tema.

O ser humano pratica condutas hodiernamente e, de acordo com o pacto social, despoja-se de parte de sua liberdade em favor da ordem social. Assim, a sociedade na qual está inserido o homem individual escolhe quais condutas devem ser punidas com mais rigor, e assim sucessivamente. Dessa forma, as condutas mais graves serão abarcadas pelo direito penal e, para as condutas intermediárias, podem-se aplicar sanções de natureza civil ou administrativa. Ainda, para a maioria da doutrina, as condutas praticadas por meio da internet geram o seu uso indevido, com a criação de condutas que espelham a necessidade de sua tipificação diante da sociedade de risco.

Nessa linha, algumas medidas estão sendo tomadas pelo Brasil.

Além disso, o Brasil foi convidado a aderir à Convenção de Budapeste em 2019 e sua validade tem o prazo de três anos.

No que se refere ao trato da matéria processual penal e da cooperação internacional, ressalta-se a importância dessas medidas para o combate da nova criminalidade transnacional e a necessidade de adoção de procedimentos uniformes contra os *cybercrime* e contra paraísos informáticos criados pela territorialidade do direito penal interno de cada Estado-membro.

Em virtude dessas considerações é possível defender a ratificação do Brasil à Convenção de Budapeste para possibilitar o alinhamento desse país aos parâmetros internacionais de combate à criminalidade transnacional, com medidas de enfrentamento a este novo cenário mundial, no contexto da quarta revolução industrial, e seus desafios cada vez mais céleres em uma velocidade exponencial jamais vista pela humanidade e ainda potencializada pelos efeitos da pandemia do COVID-19, mas sempre observando os *standarts* internacionais de direitos humanos.

Referências

ACCIOLY, Hildebrando. *Manual de direito internacional público.* 18. ed. São Paulo: Saraiva, 2010.

ALBUQUERQUE, Roberto Chacon de. *A criminalidade informática.* São Paulo: Juarez de Oliveira, 2006.

ASUÁ, Luis Jiménez. *Crônica del crimen.* Buenos Aires: Pannedille, 1970.

BRASIL, *Câmara dos Deputados*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2287513.

BRASIL Câmara dos Deputados. *Deputados e especialistas defendem adesão do Brasil a convenção sobre crimes cibernéticos.* Disponível em: https://www.camara.leg.br/noticias/772464-deputados-e-especialistas-defendem-adesao-do-brasil-a-convencao-sobre-crimes-ciberneticos/

BRASIL. Constituição de 1988. *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988.

BRASIL. Constituição de 1988. Emenda Constitucional nº 45, de 30 de dezembro de 2004. Altera dispositivos dos arts. 5º, 36, 52, 92, 93, 95, 98, 99, 102, 103, 104, 105, 107, 109, 111, 112, 114, 115, 125, 126, 127, 128, 129, 134 e 168 da Constituição Federal, e acrescenta os arts. 103-A, 103B, 111-A e 130-A, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 31 dez. 2004a.

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal. *Diário Oficial da União*, Rio de Janeiro, 31 dez. 1940.

BRASIL, *Senado Federal*. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141952.

CONSELHO DA EUROPA. *Convenção sobre o cibercrime*. Budapeste: Conselho da Europa, 2001.

COUNCIL OF EUROPE, *Convention on Cybercrime*. Disponível em: https://rm.coe.int/1680081561.

COUNCIL OF EUROPE, *Convention on Cybercrime*. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=treaty-detail&treatynum=185.

DIÁRIO OFICIAL DA UNIÃO DOU. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.

FERREIRA, Ivette Senise. *A criminalidade informática*. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). Direito & internet: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

JORNAL OFICIAL DA UNIÃO EUROPEIA, *Diretiva 2013/40/EU*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040&from=DE.

LIMA, Alceu Amoroso. *Os direitos do homem e o homem sem direitos.* Rio de Janeiro: Francisco Alves, 1974.

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

SANTOS, Denise Tanaka dos. *Os desafios da Saúde Suplementar e da Proteção de Dados Pessoais à luz da LGPD em tempos de pandemia*. *Prima@Facie*, João Pessoa, v. 20, n. 44, maio-ago., 2021, p. 311-338, DOI: https://doi.org/10.22478/ufpb.1678-2593.2021v20n44.54507.

SCHWAB, Klaus. *The fourth industrial revolution*. Geneva: World Economic Forum, 2016.