A ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE E OS IMPACTOS PARA A PRODUÇÃO DE PROVAS DIGITAIS

Marcos De Lucca Fonseca[67] *e Juliana Caramigo Gennarini*[68]

RESUMO

O presente artigo abordará os impactos que a Convenção de Budapeste tem para a produção de provas no ambiente digital, visando a coibir o Cibercrime. O Brasil aderiu ao documento após aprovação do Congresso Nacional em 15 de dezembro de 2021. Além do Brasil, a Convenção foi assinada por 66 países e, em outros 158, é usada como orientação para suas legislações nacionais. O documento criminaliza condutas, prevê normas para investigação e produção de provas eletrônicas e meios de cooperação internacional. Em apertada síntese, o texto aborda o acesso indevido e não autorizado a sistemas de computador, fraudes, material de abuso sexual infantil, violação de direitos autoriais e de segurança de redes.

PALAVRAS-CHAVE: crimes virtuais; provas digitais; Convenção de Budapeste; Marco Civil da Internet; redes sociais.

ABSTRACT

This article will address the impacts that the Budapest Convention has on the production of evidence in the digital environment, in order to curb Cybercrimes. Brazil adhered to the document, after approval by the National Congress on December 15, 2021. In addition to Brazil, the Convention was signed by 66 countries and, in another 158, it is used as a guideline for their national legislation. The document criminalizes conduct, provides rules for investigation and production of electronic evidence and means of international cooperation. In a tight summary, the text addresses improper and unauthorized access to computer systems, fraud, child sexual abuse material, copyright infringement and network security.

KEY WORDS: cybercrimes; Budapest Convention; Civil Rights Framework for the Internet; digitals evidence; social networks.

INTRODUÇÃO

A tecnologia da informação, especialmente a internet, ocasionou profundas alterações nas relações sociais dos indivíduos, trazendo novos contornos às atividades laborais, comerciais, profissionais, culturais, lazer e até às relações afetivas. Inclusive, em razão do cenário propiciado pela Pandemia do COVID-19, a digitalização e virtualização das atividades humanas cresceram exponencialmente. No Brasil, o número de horas de uso da internet para trabalho de casa passou de 3h41m para 6h44m por dia, ou seja, um aumento de três horas por dia, devido à Pandemia[69].

[67] Marcos De Lucca Fonseca**,** Perito Digital; Membro da Associação Nacional de Profissionais de Proteção de Dados Pessoais (ANPPD); Pós-graduando em Direito Digital pela Universidade Estadual do Rio de Janeiro (UERJ) – ITS; Aluno cursante da 9ª Edição do Curso de *Copyright* da Faculdade de Direito de *Harvard* em parceria com a UERL. Graduando do 9º Semestre em Direito pela Universidade Padre Anchieta (FADIPA) – Jundiaí; Graduado em Relações Internacionais pela Universidade Estadual Paulista (UNESP); Membro do Laboratório de Ciências Criminais (IBCCRIM – 2019/2020). Trabalha no setor de Telecomunicações há 10 anos.

[68] Juliana Caramigo Gennarini. Advogada criminal. Mestre em Direito Político e Econômico e Pós-graduada em Direito Penal e Processo Penal, ambas pela Universidade Presbiteriana Mackenzie. Professora Universitária em Direito Penal e Processo Penal. Coordenadora adjunta do curso de Direito e Coordenadora da Revista de Direito Penal e Processo Penal, ambos do Centro Universitário Padre Anchieta – Jundiaí/SP.

[69] Fonte: https://olhardigital.com.br/2021/05/13/coronavirus/durante-a-pandemia-consumo-de-internet-dobra-no-brasil/ Acesso em 20 em dezembro de 2021.

Somado a tal crescimento, segundo dados de pesquisa da Roland Berger, no primeiro semestre de 2021, o Brasil já tinha ultrapassado o volume de ataques cibernéticos do ano de 2020, com um total de 9,1 milhões de casos – isto levando em conta os crimes de sequestro digital (*ransomware*). Com tais números, o Brasil fica na 5ª colocação no ranking mundial, atrás de EUA, Reino Unido, Alemanha e África do Sul[70]. O cibercrime é um dos tipos de crime transnacional que mais cresce nos países membros da INTERPOL[71], e as ameaças cibernéticas estão em constante evolução, adaptando-se aos comportamentos dos usuários e às tendências online para aproveitá-las, especialmente com o aumento da utilização da internet devido ao cenário da pandemia da COVID-19.

Devido ao cenário da pandemia da COVID-19, os "cibercriminosos" diversificaram os ataques, adotando novas estratégias e utilizando-se do termo COVID-19 para impulsionar ataques. De acordo com dados da INTERPOL[72], o termo "COVID" ou "corona" foi utilizado em 2.022 domínios malignos, e em 40.261 com alto risco, o que aumenta o risco de exposição a *Malware*[73] em dispositivos telemáticos. Os "cibercriminosos" estão criando sites falsos relacionados a COVID-19, para atrair as vítimas a abrir anexos maliciosos ou clicar em links de *phishing*[74], o que leva ao sequestro de informações e dados pessoais.

Nem o recém-criado "Metaverso"[75] está imune aos cibercrimes. Em dezembro de 2021, a empresa META (nova denominação do *Facebook*[76]) abriu para usuários uma versão de teste de seu aplicativo de realidade virtual. A experiência teve a presença de 20 *avatares* que interagiram com o novo "universo", que está em fase de construção. De acordo com a empresa META, em 26 de novembro uma usuária beta

[70] Fonte: https://canaltech.com.br/seguranca/brasil-e-o-5o-maior-alvo-de-crimes-digitais-no-mundo-em-2021-195628/ Acesso em 20 de dezembro de 2021.

[71] Fonte: https://www.interpol.int/es/Delitos/Ciberdelincuencia/Desarrollo-de-Capacidades-de-Lucha-contra-la-Ciberdelincuencia/Desarrollo-de-capacidades-de-lucha-contra-la-ciberdelincuencia-en-las-Americas Acesso em 20 de janeiro de 2022.

[72] Fonte: https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19 Acesso em 20 de janeiro de 2022.

[73] Malware é um termo genérico para qualquer tipo de "malicious software" ("software malicioso") projetado para se infiltrar em dispositivos sem o seu conhecimento. Fonte: https://www.avast.com/pt-br/c-malware#gref Acesso em 20 de janeiro de 2022.

[74] Phishing é um termo originado do inglês (fishing) que em computação se trata de um tipo de roubo de identidade online. Essa ação fraudulenta é caracterizada por tentativas de adquirir ilicitamente dados pessoais de outra pessoa, sejam senhas, dados financeiros, dados bancários, números de cartões de crédito ou simplesmente dados pessoais. Fonte: https://canaltech.com.br/seguranca/O-que-e-Phishing/ Acesso em 20 de janeiro de 2022.

[75] Espaço coletivo e compartilhado na internet associado a tecnologias que recriam a experiência física no ambiente digital, formando relacionamentos que são, ao mesmo tempo, online e offline. Fonte: https://forbes.com.br/forbes-tech/2021/05/metaverso-tudo-que-voce-precisa-saber-sobre-a-tecnologia-que-integra-os-mundos-real-e-virtual/ Acesso em 20 de janeiro de 2022.

[76] Fonte: https://www.cnnbrasil.com.br/business/facebook-muda-nome-para-meta/#:~:text=Em%20meio%20%C3%A0%20crise%20do,o%20WhatsApp%20e%20a%20Oculus. Acesso em 20 de janeiro de 2022.

relatou que havia sido vítima de assédio sexual quando passou pela experiência do Metaverso[77].

Doutrinadores especialistas em Segurança Digital e Crimes Informáticos (tais como Spencer Toth Sydow e Roberto Chacon de Albuquerque) dividem os crimes informáticos em 02 grandes grupos: i) Crimes Informáticos Específicos; e ii) Crimes Informáticos Comuns. Dentro destas distinções, os Crimes Informáticos Específicos "seriam aqueles em que o sistema tecnológico é o alvo da conduta"[78] delitiva. Nesse tipo de crime, a internet é definida como um "objeto de consumo" e são adquiridos serviços de rede (tais como provedor de conexão e aplicação), e o delinquente tem a rede ou o equipamento de informática como objetivo da ação delitiva. Já os Crimes Informáticos Comuns "são aqueles em que a informática é o meio de violação de bens jurídicos"[79] . Ou seja, a informática ou a internet seria apenas o meio de adquirir ilicitamente e/ou fraudar dados pessoais e financeiros. A internet ou o equipamento informático seria apenas o meio de consumo – e não o objeto de consumo, como no caso dos crimes informáticos específicos.

Uma das mais valiosas garantias constitucionais estabelecidas em nossa Magna Carta é o Devido Processo Legal, preconizado no Artigo 5º LIV - "ninguém será privado da liberdade ou de seus bens sem o devido processo legal". Em sentido processual, basicamente, é garantir aos litigantes o acesso à justiça, igualdade de tratamento, publicidade dos atos processuais, regularidade do procedimento, contraditório e ampla defesa, realização das provas, julgamento por juiz imparcial, julgamento de acordo com provas obtidas licitamente, fundamentação das decisões judiciais etc. (NERY, 2019).

A garantia do contraditório preserva ao autor a possibilidade tanto de alegar quanto de provar os fatos que ele deduz ser de seu direito, e ao réu, de ser ouvido, poder reagir e apresentar a sua ampla defesa.

Tal garantia constitucional do contraditório judicial é pormenorizada no artigo 155 do Código de Processo Penal Brasileiro, que dispõe que o juiz não pode fundamentar a sua decisão exclusivamente nos elementos contidos na investigação criminal. As alterações promovidas pela Lei n. 13.964/2019 no Código de Processo Penal, incluindo os artigos 158-A até 158-F, positivaram os princípios básicos da cadeia de custódia da prova judicial.

A apreciação da prova, que é produzida em contraditório judicial, deve formar a sua convicção no julgamento do caso concreto. Ou seja, a prova como atividade probatória consiste

[77] Fonte: https://mittechreview.com.br/o-metaverso-ja-tem-um-problema-de-assedio-para-lidar/?utm_source=Linkedin&utm_medium=Social&utm_campaign=artigo-o-metaverso-ja-tem-um-problema-de-assedio-para-lidar Acesso em 20 de janeiro de 2022.

[78] SYDOW, Spencer Toth. Crimes informáticos e Suas Vítimas. Ed. Saraiva, 2ª Edição p. 67.

[79] SYDOW, Spencer Toth. Crimes informáticos e Suas Vítimas. Ed. Saraiva, 2ª Edição p. 68.

no conjunto de atividades de verificação e demonstração, mediante as quais se procura chegar à verdade dos fatos relevantes para o julgamento. Ocorre que até dezembro de 2021, o Brasil não havia aderido à Convenção sobre Crime Cibernético (mais conhecida como "Convenção de Budapeste"), cujo objetivo é facilitar a cooperação internacional entre os países adeptos para o combate aos crimes cometidos na internet.

Esta Convenção foi celebrada em novembro de 2001, na cidade de Budapeste (Hungria), elaborada pelo Comitê Europeu para os Problemas Criminais, e o primeiro tratado internacional sobre cibercrimes. Até junho de 2021, 66 países tinham assinado a Convenção e 158 a utilizam como orientação para suas respectivas legislações nacionais.[80]

Os principais objetivos da Convenção são criminalizar as condutas, determinar normas para investigação e produção de provas eletrônicas e meios de cooperação internacional. O presente artigo analisará as implicações, e a importância da adesão do Brasil a esta Convenção, e as consequências na investigação dos cibercrimes.

1. BREVE HISTÓRICO DOS ANTECEDENTES DA CONVENÇÃO DE BUDAPESTE

Em 13 de setembro de 1989 foi realizada a 428ª Reunião do Comitê dos Ministros dos Estados-Membros do Conselho da Europa, que publicou a Recomendação Nº R (89) 9 [81]. Este Documento, ao considerar a característica transfronteiriça da criminalidade informática e a necessidade de aumentar a cooperação jurídica internacional para combater estes delitos, recomendou aos Estados membros do Conselho da Europa revisarem suas respectivas legislações, levando em conta as recomendações do Relatório Sobre Crimes Informáticos que fora elaborado pelo Comitê Europeu. Além disso, tal Recomendação orientava sobre a importância de os Estados trocarem experiências sobre práticas judiciais para cooperação jurídica internacional sobre estes crimes.

Ainda sobre o contexto anterior à Convenção de Budapeste, em 11 de setembro de 1995 a 543ª reunião dos Ministros dos Estados-Membros do Conselho da Europa publicaram a Recomendação Nº R (95) 13, relativa à problemática de direito processual penal e tecnologia da informação[82]. Foi observado que as leis processuais penais dos Estados-Membros do Conselho da Europa tinham ausência de instrumentos investigatórios para cumprir suas tarefas, dado o contínuo desenvolvimento tecnológico do ambiente digital, principalmente

[80] Fonte: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico Acesso em 20 de janeiro de 2022.

[81] Fonte: https://rm.coe.int/09000016804f1094 . Acesso em 19 de janeiro de 2022.

[82] Fonte: https://rm.coe.int/16804f6e76 Acesso em 20 de janeiro de 2022.

quando as provas eletrônicas precisavam ser coletadas em territórios estrangeiros. Ou seja, foi destacado a necessidade dos países membros do Conselho da Europa fortalecerem a cooperação internacional, por meio de normas processuais penais compatíveis, para as investigações de crimes ocorridos na internet, bem como coleta de provas eletrônicas.

Sobre as provas eletrônicas, um dos principais avanços da Recomendação Nº R (95) 13 foi a necessidade de os países criarem normas com a finalidade de coletar, preservar e apresentar as evidências eletrônicas, de forma a assegurar a integridade e autenticidade necessária para a cadeia de custódia da prova – tanto para fins processuais em seus respectivos ordenamentos jurídicos internos, quanto para fins de cooperação internacional. Desta forma, estaria garantida a compatibilidade entre os Estados-Membros do Conselho da Europa, em matéria de provas eletrônicas. No entanto, com o objetivo de evitar possíveis violações à soberania dos Estados-Membros, foi destacada a necessidade de os Estados negociarem acordos internacionais, para balizar as condições de obtenções de tais provas.

Em novembro de 1996, o Comitê Europeu para os Problemas Criminais (CDPC) criou um comitê específico para tratar da temática da "cibercriminalidade", em termos gerais, este comitê definiu os conceitos basilares iniciais sobre os crimes que ocorrem no "ciberespaço", cujas infrações são cometidas contra a integridade, disponibilidade e confidencialidade dos sistemas informáticos e redes de telecomunicações. Um dos principais desafios, elencados desde o início dos trabalhos, foi a questão da territorialidade e o caráter transfronteiriço das infrações cometidas pela internet, e o conflito de competência com as autoridades nacionais para a aplicação da lei. Importante destacar que estas questões estavam sendo debatidas em meados da década de 90, antes do Big Data, ocorrido nos anos 2.000, que ampliou, significativamente, a utilização da internet e dos dados pessoais dos usuários.

Devido ao fato de os crimes cometidos no ambiente digital ignorarem as fronteiras das nações, o trabalho do Comitê foi um esforço de cooperação internacional para fazer frente à transnacionalidade dos delitos cometidos devido à utilização indevida dos dispositivos informáticos existente àquela época. O grande desafio foi justamente construir um instrumento jurídico que, de forma vinculativa, pudesse garantir que os Estados combatessem tais delitos – inclusive com as limitações processuais penais que os crimes transnacionais são característicos.

Um dos trabalhos deste Comitê criado pelo CPDC foi o relacionado à determinação da territorialidade do cibercrime e qual a jurisdição aplicável, evitando, assim, a ocorrência de *bis in idem*. Além disso, havia a necessidade de definir infrações penais que ocorriam no ambiente digital, especialmente aquelas cometidas nas redes das operadoras de telecomunicações

(Internet). Demais temas, como aplicações de sanções e responsabilidades no uso da internet, violações de direitos autoriais na Internet, também fora objeto de análise. Os trabalhos do Comitê resultaram em propostas de instrumentos jurídicos vinculativos, com maior ênfase nas questões internacionais relacionadas aos tópicos supra.

Em 4 de fevereiro de 1997 foi criado o "Comitê de Especialistas sobre a Criminalidade no Ciberespaço (PC-CY) que, utilizando-se do histórico dos trabalhos dos Comitês anteriores, iriam concentrar esforços para a produção de um projeto de convenção internacional sobre cibercrime. Os trabalhos deste Comitê se alongaram até o ano 2000, e finalizaram com a aprovação de um Memorando Explicativo preliminar e a revisão de um projeto de Convenção.

2. A CONVENÇÃO DE BUDAPESTE

Os objetivos centrais do documento foram, além de harmonizar os elementos do direito penal relacionados às infrações cometidas no ciberespaço, definir matéria processual interna nos países adeptos sobre investigações dos crimes cometidos por meio dos sistemas informáticos, bem como as ações necessárias para obtenção da cadeia de custódia das provas eletrônicas. Desta forma, a Convenção traz recomendações para os países que a ela aderirem criarem, ou adaptarem, em seus respectivos ordenamentos jurídicos, além de dar relevo à urgente necessidade de implantação de um regime de cooperação internacional entre os países signatários.

A Convenção está dividida em 04 capítulos, e são eles: (I) Utilização de terminologias; (II) Medidas a serem implementadas a nível nacional; (III) Cooperação Internacional; (IV) Disposições Finais. No presente artigo serão analisados apenas temas relacionados aos Capítulos II e III desta Convenção. Sobre as questões de direito penal material, a Seção 1 do Capítulo II da Convenção define 9 condutas que cada país deverá estabelecer, de acordo com o seu ordenamento jurídico interno, como infração penal. São elas:

i. Acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático;
ii. Interceptação intencional e ilegítima de dados informáticos;
iii. Interferência em dados informáticos (apagar, danificar, deteriorar, alterar ou eliminar tais dados);
iv. Interferência em sistemas, através de introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos;
v. Utilização indevida de equipamentos, essencialmente para

realização das condutas delitivas mencionadas nos itens anteriores;

vi. Falsidade informática, relacionado à produção de dados informáticos não autênticos;

vii. Perda de bens de terceiros devido à intervenções nos sistemas e dados informáticos, cujo objetivo é obter vantagem econômica para si ou para terceiros;

viii. Infrações relacionadas à pornografia infantil;

ix. Direitos autoriais

Em relação às questões de direito processual penal, que constam na Seção 2 do Capítulo II da Convenção, ocorre a divisão em cinco títulos, sendo eles:

i. Provisões comuns;

ii. Preservação antecipada de dados e de computadores armazenados;

iii. Ordem de produção;

iv. Busca e apreensão de dados armazenados em computadores;

v. Coleta de dados em tempo real e interceptação de dados;

O Capítulo III da Convenção será analisado de forma mais acurada, uma vez que ele trata das disposições relativas à assistência mútua e cooperação internacional, dividindo os temas em princípios gerais e as provisões específicas.

O Título 3 do Capítulo III da Convenção trata sobre os princípios gerais relativos ao auxílio mútuo entre os países, em matéria de investigações relacionadas às infrações penais de sistemas e dados informáticos.

A Convenção trata da assistência mútua em duas situações. A primeira relacionada à inexistência de tratado ou legislação específica recíproca entre os países para cooperação internacional em matéria de investigação penal, e as disposições da Convenção devem ser aplicadas. A segunda está relacionada ao fato de já existir uma base jurídica que possibilita a investigação entre os países, e caberá à Convenção ser aplicada igualmente a tais acordos. Uma das principais inovações da Convenção foi justamente a possibilidade de acesso transfronteiriço a dados informatizados armazenados, que não requer assistência mútua, que ocorre quando existir consentimento ou estiverem publicamente disponíveis.

Em relação à assistência mútua, de acordo com o artigo 25 da Convenção, a cooperação entre os países deve ser a mais abrangente possível, tanto para os delitos relacionados com os sistemas informáticos, quanto aqueles relacionados a acesso a dados informatizados, bem como às provas eletrônicas de outros delitos - mas sempre respeitando o ordenamento jurídico interno dos respectivos países. Destaca ainda a Convenção que a assistência mútua entre os países deve ser realizada sempre em conformidade com os

acordos, legislações e demais tratados de assistência jurídica aplicáveis, uma vez que cada Parte adotará igualmente as medidas legislativas e outras necessárias para cumprirem com tais assistências, mas cada Parte deverá dispor de uma base jurídica para poder atender às demandas de assistências mútuas relacionadas à cooperação internacional para investigação de cibercrimes. Do contrário, a assistência mútua ficaria inofensiva.

No caso de urgência, poderá uma Parte signatária solicitar à outra, mediante envio de comunicação eletrônica ou outro meio mais eficaz, a solicitação de auxílio mútuo, ou seja, sem a necessidade de emissão de cartas rogatórias entre as autoridades judiciárias dos países.

No Brasil, os artigos 783 a 786 do Código de Processo Penal dispõem sobre a necessidade de remissão de cartas rogatórias ao Ministério da Justiça, para pedido de cumprimento da carta rogatória, por via diplomática, às autoridades estrangeiras, vide:

> *Trata-se de meio de comunicação entre órgãos jurisdicionais brasileiro e estrangeiro, podendo ter por objeto a realização de citação, intimação, notificação, colheita de provas ou realização de outras diligências necessárias à instrução do processo submetido a seu julgamento (...). No entanto, se houver previsão legal em tratado firmado pelo Brasil e o país requerido (ou requerente), é perfeitamente possível a execução de medidas coercitivas no território nacional (ou estrangeiro)*[83].

Em relação às provas digitais, a celeridade para a obtenção é de suma importância, uma vez que elas são de altíssima volatilidade. Ademais, o fato de que as provas terem que ser obtidas seguindo as boas práticas da cadeia de custódia da prova relacionada à computação forense realça, ainda mais, o quanto a assistência mútua entre os países é fundamental nas investigações dos cibercrimes. Ainda sobre o processo de obtenção e acesso às provas, de acordo com o artigo 25 da Convenção de Budapeste, caberá a cada Estado definir como assegurar a validade do envio das informações solicitadas pela Parte demandante – inclusive, se necessário, adotando técnicas de boas práticas de segurança de informações, como a encriptação. De toda forma, a Convenção de Budapeste determina que cada Parte deverá dispor sobre as formas de cooperação e assistência mútua de preservação, recolha de dados em tempo real, busca e apreensão relacionadas às provas digitais.

Outro aspecto importante da Convenção é a criação de um sistema para condições e motivos de recusa para o envio das informações solicitadas pela outra Parte. Estas disposições constam no artigo 27 da Convenção, as quais

[83] DE LIMA, Renato Brasileiro. *Código de processo penal comentado*. 5ª edição. Ed. Juspodivm. 2020. p. 1671

serão analisadas pelo presente artigo, mas importa destacar que, das infrações elencadas entre os artigos 2º a 11 da Convenção de Budapeste, uma Parte não poderá recusar o envio de uma informação, alegando, para tanto, que se trata de dados de natureza "fiscal".

Um ponto que deve ser destacado é que a Parte requerida poderá condicionar a assistência mútua à existência da dupla incriminação da conduta, ou seja, o fato relacionado à obtenção das provas deve ser considerado delito em ambos os países – mesmo que a categorização da conduta delitiva esteja inserida em outra classificação de infrações, no ordenamento jurídico deste país. Do contrário, a recusa a assistência mútua poderá ser alegada pela Parte requerida.

O artigo 26 da Convenção dispõe sobre a possibilidade de as Partes atuarem na chamada "Informação Espontânea", que é justamente quando uma das Partes, ao efetuar determinada investigação de cibercrime, obtém informações relevantes de que o caso investigado poderá ser interesse da outra Parte – que, até aquele momento, não dispõe de informações sobre o referido caso. Mesmo sem o requerimento do outro Estado, aquele que possui as informações está autorizado a comunicar à outra Parte. Importa destacar que não existe uma obrigatoriedade de envio destas informações, mas sim a discricionariedade do Estado, que está em posse das informações enviar à outra Parte, se assim decidir.

3. ARTIGO 27 DA CONVENÇÃO E *FAKE NEWS*

O Capítulo 27 da Convenção de Budapeste trata dos procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis. Caso as Partes requerentes e requiridas não tiverem tais acordos internacionais, caberá a cada Parte, quando da necessidade de solicitação e envio de informações, designar quais serão as autoridades encarregadas de enviar (ou responder), executar ou transmitir os pedidos de auxílio mútuo. Mas o ponto de maior importância do artigo 27 da Convenção é que a Parte poderá recusar o pedido de assistência mútua, caso entenda que se trata de uma infração de caráter político, ou se considerar que o cumprimento de tal assistência pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial para o seu país.

Importante aqui a reflexão sobre como as Partes irão proceder no caso de uma investigação de uma conduta de divulgação de desinformação, calúnia ou difamação de (ou por) uma personalidade política. É notório que as tão faladas *fake news*, que inclusive são objeto de um Projeto de Lei nº 2630/2020[84], têm causado

[84] O PL 2630/2020, que institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, já foi aprovada no Senado Federal, e encontra-se na Câmara dos Deputados e está aguardando constituição de

grande impacto em nossa sociedade. Segundo dados do Instituto de Tecnologia de Massachusetts (MIT, sigla em inglês), o alcance das *fake news* é 70% mais veloz do que uma informação verídica. Outro dado desta mesma pesquisa é que um fato verdadeiro demora, aproximadamente, 06 vezes mais para chegar a 1.500 pessoas do que no caso de *fake news*. Se na análise for levado em consideração o reenvio de mensagens (os chamados "RTs"[85], na linguagem dos usuários das redes sociais), as falsidades atingem os demais usuários entre 10 e 20 vezes mais rápido do que os fatos verídicos[86].

Se as redes sociais, cujas plataformas e *data centers* estão localizada na maioria das vezes em territórios alienígenas, como as Partes devem proceder no caso de uma investigação de *fake news* entre personalidades políticas, ou seus respectivos partidários? Deveriam as Partes, com fundamento no artigo 27 da Convenção de Budapeste, decidir por não proceder com a assistência mútua, no caso de uma requisição? Como proceder para separar o que é fato, substancialmente político, de um crime *fake news* com finalidade eleitoral?[87] Dificilmente tal decisão não fica prejudicada sem o devido acesso às provas digitais armazenadas nos *data centers*, plataformas das redes sociais e demais provedores de aplicação da internet.

A prova digital pode ser fragmentada e separada em locais diferentes no mesmo sistema operacional. A dispersão pode ser inclusive geográfica, uma vez que os arquivos podem ser fragmentados e dispersados em várias localidades geográficas diferentes. Os próprios servidores onde as informações estão localizadas podem estar em países diferentes daqueles em que o delito ocorreu[88], uma possibilidade bem grande de ser verificada nos casos concretos de crimes contra a honra ocorridos nas redes sociais. Desta forma, é salutar que as Partes cooperem para que seja garantido o acesso à prova digital, mesmo que esta esteja localizada em território alienígena.

Evidente que, de acordo com o que prevê o parágrafo 6 do artigo 27 da Convenção de Budapeste, antes da Parte recusar o envio da requisição de assistência mútua, poderá consultar

comissão especial pela Mesa da Câmara. Fonte: https://www.camara.leg.br/propostas-legislativas/2256735 Acesso em 21 de janeiro de 2022

[85] "RT" é a abreviação da palavra "ReTweet", termo oriundo do Twitter. Na rede social, a ferramenta é usada quando um usuário deseja compartilhar em sua rede alguma mensagem interessante publicada por outra conta. Fonte: https://www.techtudo.com.br/listas/2020/06/o-que-significa-tbt-no-whatsapp-conheca-7-girias-do-app-de-mensagens.ghtml Acesso em 21 de janeiro de 2022

[86] Para acessar os dados desta pesquisa do MIT https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308 Acesso em 21 de janeiro de 2022

[87] A Lei n. 13.834, aprovada em 04 de junho de 2019 tipificou o crime de denunciação caluniosa com finalidade eleitoral, alterando o Código Eleitoral ao incluir o art. 326-A, cujo objetivo foi incriminar as chamadas "*fake news* com finalidade eleitoral". Fonte: https://revistas.anchieta.br/index.php/DireitoPenalProcessoPenal/article/view/1735/1541 Acesso em 21 de janeiro de 2022

[88] FONSECA, Marcos de Lucca. PUJOL, Sebastião Augusto de Camargo. *Perícia digital e teoria da correlação entre acusação e sentença: diferenciando fake news e calúnia nas redes sociais.* Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 2, n. 2, jul./dez. 2020. p. 26

a Parte requerente para confirmar se é possível atender apenas parcialmente o pedido, ou se propor certas condicionantes para que a cooperação seja realizada. Mas fato é que os sistemas democráticos ainda não decidiram como irão tratar os temas relacionados à moderação de conteúdo na internet, principalmente quando o conteúdo é divulgado por personalidades ou ativistas políticos, e com indícios de ser considerado como *fake news*.

4. A CONSERVAÇÃO DOS DADOS ARMAZENADOS: CONVENÇÃO DE BUDAPESTE E O MARCO CIVIL DA INTERNET

A Convenção de Budapeste, em seu artigo 29, discorre sobre a conservação dos dados informáticos armazenados. Ele dispõe que a Parte requerente solicite à requirida a manutenção de determinados dados informáticos, uma vez que a Parte requisitante prevê solicitar um pedido de auxílio mútuo de busca, acesso, apreensão, ou obtenção por meio similar ou divulgação sobre tais dados.

Vejamos as implicações do artigo 29 da Convenção em relação à lei federal brasileira nº 12.965/2014 (Marco Civil da Internet). De acordo com o artigo 13 do Marco Civil da Internet,

> *Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.*
> *(...)*
> *§ 2º § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.*

Ou seja, caso uma Parte solicitar ao Brasil dados informáticos de um provedor de conexão à internet[89] localizado no território nacional, e estes dados estiverem no prazo superior a 01 (hum) ano, tal pedido da Parte requisitante poderá estar prejudicado, uma vez que os provedores de conexão localizados no território brasileiro não têm obrigatoriedade de manter tais dados por prazo superior.

Vamos a um caso hipotético. Se um estrangeiro natural de um país que é Parte da Convenção de Budapeste, ao acessar um *website* de um provedor de aplicações[90] brasileiro, e for vítima de um cibercrime devido a uma falha no sistema de segurança da informação deste provedor, caso a autoridade estrangeira solicitar ao seu par brasileiro acesso mútuo para conhecer,

[89] De acordo com o art. 5º, V do Marco Civil da Internet, considera-se conexão à internet *"(...) V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;* Ex: operadoras de telecomunicações

[90] De acordo com o art. 5º, VII do Marco Civil da Internet, considera-se conexão internet *"*(...) VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet*"*. Ex: redes sociais; plataformas de *marketplaces*

por exemplo, os dados informáticos de registro de conexão[91] do provedor de conexão para obter o número do IP (*Internet Protocol*)[92], e tal solicitação for há mais de 01 (hum) ano do caso objeto da investigação, o provedor de conexão brasileiro não tem a obrigação de fornecer tais dados.

Mesmo que o art. 13, §2º do Marco Civil da Interne preveja que "(...) A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput (...)" – ou seja, pelo prazo superior a 01 (hum) ano, a requisição do caso hipotético supra teria que ocorrer antes deste prazo. Logo, a Parte requisitante deveria solicitar a assistência mútua à autoridade brasileira em um lapso temporal, em que esta pudesse redirecionar ao provedor de conexão dentro do prazo de 01 (hum) ano - mesmo que aquela (a Parte requisitante) solicitasse apenas a manutenção/conservação dos dados informáticos (como determina o artigo 29 da Convenção da Budapeste).

Isto porque, de acordo com o artigo 11 do Marco Civil da Internet, qualquer operação de coleta, armazenamento, guarda e tratamento de registros de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros – desde que os dados coletados em território nacional e o conteúdo das comunicações estejam, pelo menos um dos terminais, localizados no Brasil. E como a própria Convenção de Budapeste dispõe que as legislações internas dos respectivos países Parte devem ser mantidas, o Marco Civil da Internet deve ser respeitado.

Um aspecto importante que precisa ser destacado foi a recém decisão da 6ª Turma do Superior Tribunal de Justiça, que deliberou que é válido o pedido de congelamento de dados telemáticos antes da autorização judicial[93]. No caso, foi considerado válido o pedido feito pelo Ministério Público – sem autorização judicial – para que provedores de internet congelassem dados telemáticos de usuários, preservando-os para fins de investigação criminal. A defesa

[91] De acordo com o art. 5º, VI do Marco Civil da Internet, considera-se conexão internet "(...) VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;"

[92] O IP é uma expressão bastante popular, embora nem todo mundo saiba exatamente o seu significado. O termo é a sigla para Protocolo da Internet, ou Internet Protocol, em inglês. Esse protocolo funciona de forma semelhante ao CPF de uma pessoa física, permitindo que conexões e dispositivos sejam identificados a partir de uma sequência numérica. Fonte: https://canaltech.com.br/software/o-que-e-ip/ Acesso em 21 de janeiro de 2022

[93] https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/18022022-E-valido-pedido-de-congelamento-de-dados-telematicos-antes-de-autorizacao-judicial--decide-Sexta-Turma.aspx. Acesso em 15 de abril de 2022

sustentou a tese de nulidade das provas obtidas por meio da quebra de dados telemáticos, uma vez que o *Parquet* teria, antes de apresentar um pedido à autoridade judicial, enviado ofícios às empresas Apple e Google, a fim de impedir a livre disposição, por parte de seus titulares, dos dados telemáticos que estivessem armazenados com elas.

No entendimento do relator, o Marco Civil da Internet tornou mais eficiente o acesso a dados para fins de investigação criminal, ao possibilitar que o Ministério Público requeira diretamente ao provedor a sua guarda, em ambiente seguro e sigiloso, evitando o descarte dos conteúdos pelos usuários, vide:

> *O pedido de congelamento do Ministério Público, contra o qual se rebelam os impetrantes, e diversamente do que advogam, não precisa necessariamente de prévia decisão judicial para ser atendido pelo provedor, mesmo porque – e esse é o ponto nodal da discussão, visto em face do direito à preservação da intimidade, da vida privada, da honra e da imagem das partes (artigo 5º, X, da Constituição Federal e artigo 10 da Lei 12.965/2014) - não equivale a que o requerente tenha acesso aos dados congelados sem ordem judicial.*

No entendimento do relator, o congelamento do conteúdo telemático nos provedores de internet recebe tratamento específico da Lei 12.965/2014, que afirma ser dever jurídico do administrador do respectivo sistema autônomo manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano; e, no caso do provedor de aplicações de internet, pelo prazo de seis meses.[94]. A autoridade policial ou administrativa, ou, ainda, o Ministério Público, poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto, devendo, em até 60 dias após o requerimento, ingressar com o pedido de autorização judicial para o acesso aos registros (artigos 13 e 15 da Lei 12.965/2014).

Por fim, ponderou o magistrado que quanto à disponibilização dos conteúdos, "(...) deve sempre ser precedida de autorização judicial devidamente fundamentada, o que ocorreu no presente caso".

CONCLUSÃO

O objetivo do presente artigo foi trazer à luz do debate os impactos que a Convenção sobre Cibercrime (Convenção de Budapeste, da qual o Brasil ratificou sua adesão em dezembro de 2021) terá sobre o ordenamento jurídico brasileiro. A adesão do Brasil à esta Convenção é de fundamental importância, uma vez que garante maior celeridade para a cooperação internacional nas atividades relacionadas à

94 https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/18022022-E-valido-pedido-de-congelamento-de-dados-telematicos-antes-de-autorizacao-judicial--decide-Sexta-Turma.aspx. Acesso em 15 de abril de 2022

persecução penal dos crimes cometidos no ambiente digital.

Evidente que a cadeia de custódia da prova dos crimes digitais requer atividades especializadas de computação forense e perícia digital. Fato é que, devido às estratégias comerciais das empresas de tecnologia e segurança da informação, as informações relacionadas às possíveis evidências digitais nem sempre estão localizadas no mesmo país em que tais crimes ocorrem. Logo, a cooperação internacional entre os Estados é de fundamental importância para garantir que o acesso às provas, bem como as garantias do direito ao devido processo legal, contraditório e ampla defesa, sejam exercidas nos processos judiciais – em especial no direito processual penal, evitando, assim, a punição de eventuais inocentes e a impunidade de culpados por tais crimes digitais.

Por outro lado, é necessário que os países, ao aderirem à esta Convenção, procedam com os ajustes necessários em seus respectivos ordenamentos jurídicos, evitando, assim, o conflito aparente das normas infraconstitucionais com os dispositivos da Convenção de Budapeste.

Evidente que o texto da própria Convenção dispõe que as normas infraconstitucionais devem prevalecer frente a este conflito de normas – tal como abordado no texto do presente artigo. Mas esta situação de conflito de normas poderá suscitar um cenário de insegurança jurídica, como no caso do prazo máximo necessário para a manutenção das informações sobre a operação de coleta, armazenamento, guarda e tratamento de registros de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet (em que pelo menos um desses atos ocorra em território nacional), caso a persecução penal de um crime digital, ocorrido em outro país, demore além do prazo estipulado no Marco Civil da Internet brasileiro. Sendo assim, caberá às autoridades judiciárias brasileiras alertarem os legisladores quanto à esta possibilidade, bem como sobre potencial atualização legislativa para adequar a legislação brasileira para esta realidade normativa, que resultou com a adesão do Brasil à Convenção de Budapeste.

De fato, os crimes cometidos no ambiente digital, principalmente os cometidos na internet, cresceram de forma substancial desde a década de 1990 - e de forma vertiginosa, com o *Big Data*, a partir dos anos 2000. Uma das necessidades dos países membros do Conselho Europeu foi, desde as Recomendações oriundas das reuniões dos Comitês de Ministros, criar regulamentações para obtenção dos dados informáticos obtidos no ambiente cibernético. A Convenção de Budapeste foi o resultado da construção destes trabalhos, desde o fim da década de 1980 e meados dos anos 1990.

A Convenção de Budapeste é de fundamental importância para a assistência mútua entre as Partes, especialmente no que diz respeito à obtenção de provas digitais dos crimes

cibernéticos – ainda mais no cenário atual, em que as redes sociais, e utilização de plataformas digitais na internet, tornaram-se uma potente ameaça à Democracia, ao Estado Democrático de Direito, e aos valores republicanos, ainda mais na propagação de desinformação sobre a triste realidade da pandemia da COVID-19.

De toda forma, como a própria Convenção de Budapeste dispõe, os Estados devem exercer a cooperação internacional - no que diz respeito às atividades de investigações dos crimes cometidos no ambiente digital – sem ameaçar seu ordenamento jurídico pátrio. Evidente que isto não resulta em um cenário de ausência de assistência mútua entre os países signatários, mas a questão da cooperação internacional para as investigações dos cibercrimes perpassa a atuação estatal, ou seja, cabe aos agentes privados – como as redes sociais e as plataformas digitais – estabelecerem medidas que colaborem na obtenção das provas digitais, independentemente da localização geográfica em que estas se encontram. Do contrário, corre-se o risco do ordenamento jurídico interno dos países, ao garantir o devido processo legal e demais garantias constitucionais do contraditório e ampla defesa, servir de justificativa jurídica para que tais agentes privados não forneçam informações que podem, substancialmente, colaborarem com a resolução dos crimes que ocorrem no ambiente digital – especialmente devido à grande utilização das redes sociais.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXY, Robert. *Teoria dos direitos fundamentais.* 2 ed. São Paulo: Malheiros, 2017.

ASTURIANO, Gisele. *Direito à imagem na internet e a responsabilidade civil:* A (re) significação do homo virtualis. São Paulo: Boreal, 2017.

BAUMAN, Z. RAUD, Reins. *A individualidade numa época de incertezas. ed. Zahar. 2015*

BULOS, Uadi Lammêgo. *Curso de direito constitucional.* 11 ed. São Paulo: Saraiva, 2018.

CASTELLS, Manuel. *A sociedade em rede.* São Paulo: Paz e Terra. 2018

COLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos.* Ed. Juruá. 2010

COLNAGO, Cláudio de Oliveira Santos. *Liberdade de expressão na internet.* ed. JusPodivm

_____. *Os direitos da personalidade no código civil.* ed. Renovar. *2002.*

DECRETO LEGISLATIVO Nº 37/2021, que aprovou o texto da Convenção sobre o crime cibernético, celebrada em Budapeste, em 23 de novembro de 2001.

https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/12/2021&jornal=515&pagina=7&totalArquivos=188.

FRAJHOF, Isabella Z. *O direito ao esquecimento na internet*. ed. Almedina. 2019.

FRAZÃO, Ana. MULHOLLAND, Caitlin. *Inteligência artificial e direito*. SP: RT. 2019.

GONÇALVES, Diogo Costa. *Pessoa e direitos de personalidade. Fundamentação ontológica da tutela*. ed. Almedina. 2008.

LIMA, Renato Brasileiro de. *Código de processo penal comentado*. Ed. Juspodivm. 2020

MORAES, Maria Celina Bodin de. KONDER, Carlos Nelson. *Casos e decisões sobre os novos desafios para a tutela da pessoa humana nas relações existenciais.*

MORAES, Maria Celina Bodin de. *Na medida da pessoa humana. Estudos de direito civil-constitucional*. ed. Processo. 2016.

SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. Ed. Saraiva. 2ª edição. 2015