OBSERVATÓRIO DA LGPD
UNIVERSIDADE DE BRASÍLIA

ANÁLISE SETORIAL
IMPACTOS DA LGPD NO BRASIL

ORGANIZADORES

LAURA SCHERTEL MENDES

GIOVANNA MILANESE

PAULO RICARDO DA SILVA SANTANA

SHANA SCHLOTTFELDT

TAYNÁ FROTA DE ARAÚJO

EDUARDA COSTA ALMEIDA

ELIS BANDEIRA A. BRAYNER

ANUÁRIO DO OBSERVATÓRIO DA LGPD DA UNIVERSIDADE DE BRASÍLIA

VOLUME 2

Universidade de Brasília
Faculdade de Direito

Anuário do Observatório da LGPD da Universidade de Brasília

Análise setorial dos impactos da LGPD no Brasil

Volume 2
Brasília-DF
2023

Para esclarecimentos sobre esta obra, entrar em contato com observatorio.lgpd.unb@gmail.com

Volume 2

Organização
Coordenação Geral: prof.ª Laura Schertel Mendes;
Coordenação Adjunta: Giovanna Milanese;
Coordenação de Pesquisa: Paulo Ricardo S. Santana e Shana Schlottfeldt;
Assessores da Coordenação de Pesquisa: Igor M. Caldas Machado, Luís Fernando O. S. Costa, Sayuri Hamaoka e Sofia de M. Vergara;
Revisão e Organização: Eduarda Costa, Elis Bandeira A. Brayner e Tayná Frota de Araújo.

Informações

Observatório da LGPD/Unb
Faculdade de Direito
Universidade de Brasília
Campus Universitário Darcy Ribeiro, CEP: 70.910-900, Brasília-DF, Brasil

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Central da Universidade de Brasília – BCE/UNB)

A636 Anuário do Observatório da LGPD da Universidade de Brasília [recurso eletrônico] : análise comparada entre elementos da LGPD e do GDPR / organização Laura Schertel Mendes … [et al.]. – Brasília : Universidade de Brasília, Faculdade de Direito, 2024. 2 v.

Inclui bibliografia. Modo de acesso: World Wide Web.

ISBN 978-65-00-92398-8 (v. 1).

ISBN 978-65-00-92399-5 (v. 2).

1. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 2. Universidade de Brasília. 3. Proteção de dados. 4. Direito comparado. I. Mendes, Laura Schertel (org.).

CDU 34

AUTORES

André Felipe Krepke

Camila Cristina da Silva

Elis Bandeira Alencar Brayner

Gustavo Vieira de Sousa

Igor Marques Caldas Machado

Isabella Maria Farias Carvalho

Lívia Rodrigues Alves

Luis Eduardo de Souza Leite Trancoso Daher

Luís Fernando Oliveira de Souza Costa

Paulo Ricardo da Silva Santana

Rafaella Bacellar Marques

Rodrigo Toledo Costa de Almeida

Sofia de Medeiros Vergara

Tayná Frota de Araújo

Thobias Prado Moura

Wanessa Larissa Silva de Araújo

REVISORES

A realização deste anuário contou com a significativa participação de revisores, que atuaram na avaliação e revisão dos artigos submetidos pelos pesquisadores do Observatório, fornecendo orientações e sugestões de melhoria. Oferecemos nosso mais sincero agradecimento pelas valiosas contribuições de cada um.

Cynthia Picolo

Eduarda Chacon

Eduarda Costa

Felipe Medon

Gabriel Fonseca

Giovanna Milanese

Isabela Maria Rosal

Maria Cristine Lindoso

Matheus Pimenta

Mônica Fujimoto

Rodrigo Silva

Thiago Moraes

SUMÁRIO

ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE

Elis Bandeira Alencar Brayner[1]

Resumo: Em 30 de novembro de 2022, o processo de adesão do Brasil à Convenção de Budapeste foi concluído, de modo a alterar o panorama nacional de repressão a crimes cibernéticos. A partir desse contexto, o presente trabalho buscou realizar revisão bibliográfica sobre a Convenção sobre Crimes Cibernéticos, compilar a legislação brasileira acerca do Direito Digital pré-existente e verificar a compatibilidade entre ambos. Adiante, foi realizada uma análise do contexto histórico no qual foi criada a Convenção de Budapeste, seu conteúdo, a posição hierárquica dos tratados internacionais no Brasil e das normas de controle de delitos no meio virtual. Observou-se que há estreita harmonia entre as normas internas e a Convenção sobre Crimes Cibernéticos e, mais que isso, a adesão do Brasil representa um avanço na responsabilização penal de agentes que praticam condutas criminosas na internet.

Palavras-chave: crimes cibernéticos; Convenção de Budapeste; Direito Digital; internet.

Abstract: *On November 30, 2022, the Brazilian adhesion process to the Budapest Convention was concluded, thus changing the national framework of repressing cybercrime. Within this scenario, this paper seeks to conduct a literature review on the Convention on Cybercrime, compile the pre-existing Brazilian legislation on Digital Law and verify the compatibility between the two. Furthermore, an analysis of the historical context in which the Budapest Convention was created, as well as its content, the hierarchical position of international treaties in Brazil and the rules of crime control in the virtual environment was performed. The study observed that there is a strong harmony between the domestic norms and the Convention on Cybercrime and, moreover, Brazil's adhesion represents an advance in the criminal liability of agents who practice criminal conducts on the internet.*

[1] Elis Bandeira Alencar Brayner é pós-graduanda em Direito Digital e Proteção de Dados do Instituto Brasiliense de Direito Público (IDP). Bacharela em Direito pela Universidade de Brasília (UnB). Pesquisadora do Privacy Lab - Centro de Direito, Internet e Sociedade (CEDIS) do IDP. Coordenadora de Comunicação do Observatório da LGPD/UnB. Estagiária da Pós-Graduação da Defensoria Pública da União no 5º Ofício Cível. Advogada.

***Keywords*:** *cybercrimes; Budapest convention; Digital Law; internet*

Introdução

Em 21 de novembro de 2001, foi aberta para assinatura, em Budapeste, a Convenção do Conselho Europeu sobre o Cibercrime, o primeiro acordo internacional que tratou explicitamente sobre essa espécie de crimes, também conhecida como Convenção de Budapeste. Este tratado entrou em vigor apenas em 2004 (COUNCIL OF EUROPE, 2017, *online)* e possui como objetivo principal:

> (...) a repressão dos crimes cibernéticos com a utilização de normas eficientes e práticas, mediante as quais a sociedade se sinta segura para se desenvolver, sem a interferência daqueles que procuram por meios escusos conseguir lucros, mesmo que causem prejuízos monetários e danos morais a terceiros. (FERNANDES, 2013, p.175)

Durante a convenção de Budapeste, o espaço cibernético foi definido como um espaço comum utilizado por aqueles que trafegam na internet a partir da conexão com os serviços de comunicação e informação (BOITEUX, 2004, p. 170). Ou seja, é nesse ambiente que os crimes cibernéticos ou cibercrimes ocorrem.

Os crimes digitais tornaram-se progressivamente mais relevantes e perigosos com a evolução da tecnologia da informação, que estão presentes na rotina de indivíduos espalhados por todo o globo. De acordo com dados de um relatório da União Internacional de Telecomunicações, em 2022, 67% da população mundial estava conectada à internet.

Dentre os casos recentes de crimes virtuais no Brasil com repercussão nacional, cita-se o ataque ocorrido em novembro de 2020 ao sistema eletrônico do Superior Tribunal de Justiça que resultou no bloqueio de acesso aos processos que tramitam na egrégia corte e aos e-mails de seus funcionários (ALVES, Paulo, 2020, n.p.). Até o presente momento, as investigações do referido crime ainda não foram concluídas pela Polícia Federal.

Nesse contexto, buscar-se-á analisar o disposto no ordenamento jurídico brasileiro acerca do Direito Digital e na Convenção de Budapeste, à qual o Brasil aderiu no final de 2022. Esse artigo dedica-se a averiguar se, de fato, houve algum benefício com a adesão ao tratado internacional.

1. A Convenção de Budapeste e a tipificação penal de crimes cibernéticos

O primeiro registro da utilização do termo "crime cibernético" ocorreu em 1997, antes mesmo da Convenção de Budapeste, em 1997, durante um encontro dos líderes do G-8, grupo formado pelos países considerados mais desenvolvidos econômica e industrialmente, responsável pela adoção dos Dez Princípios do Combate ao Cibercrime (ANTUNES, 2022, p. 25). Esse termo continua sendo atual e utilizado pela literatura dedicada ao tema e, de acordo com as lições de NASCIMENTO (2021, n.p.), pode ser definido como:

> (...) todas as condutas típicas, antijurídicas e culpáveis praticadas no âmbito digital ou que estejam envolvidas com a informação digital através dos mais diversos meios e dispositivos conectados à internet, tais como computadores, celulares, smartphones e tablets. Estes crimes se propagam através da internet, em razão das diversificadas maneiras de interação entre indivíduos que surgiram ao longo do tempo.

O texto Convenção de Budapeste é formado por 48 artigos, que se organizam em quatro capítulos, quais sejam: *I) Terminologia*; *II) Medidas a Tomar a Nível Nacional*; *III) Cooperação Internacional;* e *IV) Disposições Finais*, respectivamente. Nele, o cibercrime foi tipificado como infrações contra sistemas e dados de tecnologias da informação (Capítulo II, Título I), infrações relacionadas com computadores (Capítulo II, Título II), infrações relacionadas com o conteúdo, como a pornografia infantil (Capítulo II, Título III) e infrações relacionadas com a violação de direitos autorais (Capítulo II, Título IV), cujas proposituras estão adentradas em Direito Penal Material (CONVENÇÃO DE BUDAPESTE, 2001).

Hoje, o Tratado possui 68 países signatários do Tratado, que também é utilizado por outros 156 países como fonte de orientação em suas legislações nacionais (COUNCIL OF EUROPE, 2017, *online)*. A seguir, serão detalhados o contexto histórico no qual surgiu esse documento, seu conteúdo e a posição hierárquica dos tratados internacionais no ordenamento jurídico brasileiro.

1.1. Contexto histórico

A primeira tentativa de harmonizar as leis sobre crimes cibernéticos ocorreu na Europa em 1989, por meio da publicação de diretrizes para os legisladores dos Países-membros do Conselho Europeu, denominada Recomendação R(89)9.

Essas orientações consistem numa lista de oito infrações específicas relativas a computadores, sendo elas: fraude informática, falsificação informática, danos a dados ou programas de computador, sabotagem informática, acesso não autorizado, interceptação não autorizada, reprodução não autorizada de uma topografia. A referida lista era composta ainda por quatro delitos facultativos: alteração de dados ou programas de computador, espionagem de computador, uso não autorizado de um computador, uso não autorizado de um programa de computador protegido (GROTTO, 2010, p. 4).

Não obstante, em 1997, a União Europeia constatou em relatório que as diretrizes da Recomendação R(89)9 não haviam alcançado a compatibilização visada. Isto é, a despeito da recomendação, as Nações-membros do Conselho Europeu continuavam com discrepâncias expressivas quanto às suas legislações sobre crimes virtuais, de modo a se fazer imprescindível a criação um tratado que permitisse uma cooperação internacional efetiva e harmônica (GROTTO, 2010, p. 5), nas palavras de um dos membros do Conselho Europeu, Dr. Henrik Kaspersen (KASPERSEN, 1997, p. 104 a 106):

> (...) há Estados-membros que não implementaram (a Recomendação) de modo algum, enquanto outros apenas implementaram um certo número de diretrizes ou não seguiram determinada diretriz pertinente ao caso.

No ponto, insta destacar que a harmonia de leis acerca de crimes cibernéticos é essencial, haja vista que a falta de dupla criminalidade, por exemplo, impede que as investigações que envolvem vários países tenham sucesso (GARCIA, 2004, PICOTTI, 2005, n.p.). Sendo assim, em novembro de 1996, o Comitê Europeu para Problemas Criminais reuniu um conjunto de especialistas para que um tratado internacional fosse instituído de forma a solucionar a questão dos crimes digitais (CSONKA, 2004, p. 247).

O resultado desse encontro de especialistas é precisamente a Convenção de Budapeste, que foi assinada de imediato por 26 Estados-membros do Conselho Europeu e quatro Estados

não membros que participaram ativamente da redação do tratado internacional, quais sejam Estados Unidos, Canadá, Japão e África do Sul (COUNCIL OF EUROPE, 2017, *online)*.

1.2. A Convenção de Budapeste

Produto de quatro anos de trabalho intenso do comitê de especialistas em cibercrimes, a Convenção de Budapeste foi responsável por (i) estabelecer o conceito de certos delitos virtuais, possibilitando definições comuns entre diferentes nações; (ii) definir regras acerca de poderes investigativos e de persecução penal e; (iii) determinar formas de cooperação entre países, tanto tradicionais quanto novas, acelerando e tornando mais efetiva a investigação de delitos (BOITEUX, 2004, p. 170). A seguir, serão examinadas cada uma dessas melhorias previstas neste tratado internacional.

A primeira parte da Convenção de Budapeste dedica-se a definir e tipificar o cibercrime, possibilitando a dupla criminalidade, ou seja, que a conduta seja considerada um delito em mais de um país e possa haver uma organização no combate à criminalidade transnacional (ALVES, 2018, p. 11). Salienta-se que todos os crimes previstos no tratado são dolosos, em outras palavras, apenas são punidas as condutas em que o agente teve a intenção de produzir o resultado ou assumiu o risco de produzi-lo (BOITEUX, 2004, p. 171). Os delitos previstos no tratado se amoldam em quatro categorias diferentes.

O tratado prevê como categoria inicial as "ofensas contra a confidencialidade, integridade e disponibilidade de dados ou sistemas de informação" (CONVENÇÃO DE BUDAPESTE, 2001). São inseridos nessa categoria os delitos que possuem como alvo o sistema informático ou os dados, ligados intrinsecamente ao ambiente informático no qual ocorrem (CSONKA, 2004, p. 22).

A segunda categoria de delitos abrange as versões computadorizadas de fraude e falsificação, que consistem essencialmente em manipulações de *input* (entrada), ou seja, dados incorretos inseridos no espaço virtual por manipulação de programas ou interferências no processamento de dados (CSONKA, 2004, p. 27).

A terceira categoria é aquela relativa à pornografia infantil, que foi considerada pelo Conselho Europeu como uma das mais perigosas (COUNCIL OF EUROPE, 2000, n.p.).

A quarta e última categoria de infrações refere-se às violações de direitos autorais e afins por meio de redes de computadores. No ponto, sublinha-se que as infrações aos direitos

de propriedade intelectual são as que mais comumente são cometidas na internet, podendo causar danos substanciais (CSONKA, 2004, p. 32).

No que tange à segunda parte da Convenção de Budapeste, que define os poderes investigativos e de persecução penal, o tratado lida com: preservação acelerada de dados de computador armazenados; conservação e divulgação parcial de dados de tráfego; ordem de produção; consulta de sistemas computadorizados; apreensão de dados de computador armazenados; levantamento de dados de tráfego em tempo real e; interceptação de dados de conteúdo (CSONKA, 2004, p. 32). Essa seção viabiliza a repressão de crimes informáticos.

A parte final da Convenção busca implementar um procedimento de cooperação internacional célere e concreto, que deve ocorrer "da forma mais extensa possível" (CONVENÇÃO DE BUDAPESTE, 2001). Uma inovação considerável prevista é a criação da base legal relativa a uma rede internacional de assistência específica ao crime informático, uma estrutura de pontos de contato nacional disponível permanentemente, "rede 24/7" (CSONKA, 2004, p. 48).

1.3. *Status* dos tratados internacionais no Direito brasileiro

Antes de adentrar no tema da adesão do Brasil à Convenção de Budapeste, é importante compreender a posição que os tratados internacionais ocupam na hierarquia das normas do Direito brasileiro.

Apesar de serem hierarquicamente inferiores à Constituição Federal brasileira[2], de sorte a não poderem dela divergir, os tratados internacionais posicionam-se em nível superior ao das leis ordinárias e complementares, pois, consoante preceituado João Bosco Lee "para que uma regra de direito internacional possa ser eficaz no território do país que ratificou o tratado, deve essa regra prevalecer sobre o direito interno" (BORGES, 2007, p. 230).

Da mesma maneira, o artigo 27 da Convenção de Viena sobre o Direito dos Tratados, firmada em 23 de maio de 1969, estabelece que um país não pode utilizar suas normas de direito interno "para justificar o inadimplemento de um tratado". Sublinha-se que o Brasil se

[2] Ressalvados aqueles que versarem sobre direitos humanos e que forem aprovados sob o rito previsto no art. 5º, §3º da Constituição Federal, os quais possuem status de emenda constitucional.

comprometeu, em 14 de dezembro de 2009, a cumprir essa convenção por meio do Decreto nº 7.030.

O Direito Internacional Público consiste no conjunto de normas autônomas que guiam as relações entre Estados soberanos, sendo os tratados os instrumentos responsáveis pela estruturação dessas relações, disciplinando as condutas entre diferentes nações. Em conformidade com as lições de REZEK (2000, p.14), "Tratado é todo acordo formal concluído entre sujeitos de direito internacional público, e destinado a produzir efeitos jurídicos".

Nesta oportunidade, explica-se resumidamente o rito de incorporação dos tratados internacionais ao ordenamento jurídico brasileiro, após as negociações entre os países, assim como disposto na Constituição Federal. No Brasil, como regra geral, o texto original é enviado ao Congresso Nacional, sendo discutido inicialmente na Câmara dos Deputados e, caso aprovado, seguindo ao Senado Federal (FLORIANI, 2019, p. 255 e 256).

Havendo aprovação nas duas casas do Congresso Nacional, o presidente do Senado promulga um Decreto Legislativo acerca da aprovação do texto do tratado, que deve ser analisado pelo Poder Executivo para definir se este tratado será ratificado ou não (BRASIL, CF, Senado, 1988). Frisa-se que o Poder Executivo não possui prazo ou obrigatoriedade de ratificar o tratado internacional, sendo um ato discricionário (FLORIANI, 2019, p. 256).

Em uma sociedade globalizada, o instrumento dos tratados internacionais ganha cada vez mais relevância. Quando se considera os crimes cibernéticos, essa afirmação é ainda mais palpável, pois o mundo virtual é capaz de romper fronteiras nacionais e integrar localidades fisicamente distantes (PINHEIRO, 2007, p. 45).

2. Crimes digitais no Brasil

A prática de crimes cibernéticos tem crescido com o desenvolvimento da Era da Informação em todo o mundo. De acordo com projeções realizadas pelo Fórum Econômico Mundial, os custos globais decorrentes desses delitos em 2023 serão de 8 trilhões de dólares e, em 2025, 10.5 trilhões de dólares. Hoje, se comparado às maiores economias do globo, o cibercrime representaria, em números, a terceira maior economia do mundo, atrás apenas dos Estados Unidos e da China (WORLD ECONOMIC FORUM, 2023).

O Brasil está incluído nessa tendência. Segundo dados fornecidos pelo diretor da Confederação Nacional de Seguradoras (CNseg), Alexandre Leal, o país foi o segundo país que

mais sofreu com crimes cibernéticos em 2022: foram aproximadamente cem bilhões de tentativas de ataques cibernéticos, número de ocorrências apenas menos do que o do México, no qual foram detectadas 187 bilhões de tentativas (FIDESRJ, 2023). Destarte, considerando que o Estado possui como função proteger os bens jurídicos fundamentais para a vida em sociedade, exercendo o monopólio do Direito Penal, a tipificação de crimes cibernéticos se revela essencial (JESUS, 2014, p. 46).

Iniciado em junho de 2018, o processo de adesão do Brasil à Convenção de Budapeste foi concluído em 30 de novembro de 2022, quando o País, em conjunto com o Conselho Europeu, depositou sua carta de adesão à Convenção de Budapeste (GOV, 2022). O próximo capítulo pretende estudar as leis já instituídas no Brasil acerca dos crimes digitais e os aspectos de sua adesão a esse tratado internacional.

2.1. Compilado legislativo nacional

O ordenamento jurídico brasileiro, até o presente momento, apresenta apenas três leis que tutelam os conflitos advindos da má utilização da internet: a Lei Carolina Dieckmann (Lei 12.737/12), a Lei Azeredo (Lei 12.735/12) e o Marco Civil da Internet (Lei 12.965/14), que altera o Código Penal (COLTRO, 2021, p. 108). As duas primeiras leis foram criadas a partir de situações específicas que resultaram em forte comoção social.

A Lei 12.737/2012 originou-se do fato de Carolina Dieckmann, atriz de renome nacional, ter sido vítima de invasão em seu computador com a consequente publicação de 36 fotos íntimas suas na internet. Em razão da rápida e significativa repercussão midiática do fato, alguns especialistas afirmam que a lei foi aprovada em regime de urgência, sem tempo hábil para o adequado debate sobre o tema em pauta, fato que teria resultado em uma norma com previsões excessivamente abertas e lacunas de definições técnicas imprecisas (CIDRÃO, 2018, p. 72). Confira-se, *in verbis*, a conduta tipificada:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

> § 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 .
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I – Presidente da República, governadores e prefeitos;
> II – Presidente do Supremo Tribunal Federal;
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Os críticos desse diploma legal, majoritariamente, consideram insuficiente a pena máxima estabelecida para o delito, que viabiliza a adoção do rito sumaríssimo dos juizados especiais e, por consequência, facilita "a suspensão condicional do processo, a conciliação, a composição civil dos danos e a transação penal" (GARCIA, 2017, p. 51). Ademais, o fato de a pena ser breve também resulta em curto prazo de investigação do delito, fazendo com que diversos crimes não sejam punidos em razão da prescrição (LIRA, 2014, p. 66).

De seu lado, a Lei Azeredo recebeu este nome em razão do autor do seu projeto (PL nº 84/1999) o Senador Eduardo Azeredo. O Projeto de Lei tipifica treze condutas como crimes virtuais, incluindo (COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA, 2006, p. 4):

> (...) obrigar a todos os que desejarem acessar uma rede de computadores a identificar-se e cadastrar-se. Do outro lado, pretende obrigar a todos os que dispõem de rede a somente admitir como usuário pessoa ou dispositivo de comunicação ou sistema informatizado que seja autenticado consoante validação positiva dos dados cadastrais

> previamente fornecidos, mediante contrato formalizado perante o fornecedor do serviço.

O PL nº 84/1999, à época em que foi apresentado, recebeu o apelido de "AI5 Digital" pela bancada do Partido dos Trabalhadores que o acusava de "incitar a criação de um estado policial na internet" (MOLITOR, 2017, p. 89).

Em seus quase 13 anos de tramitação, o projeto original sofreu diversas alterações e cortes, resultando na Lei 12.735/12, nota-se que sua publicação ocorreu no mesmo ano da Lei Carolina Dieckmann, após a grande repercussão do vazamento de fotos íntimas da atriz. Em sua versão final, a lei aprovada levantou apenas dois pontos (MOLITOR, 2017, p. 90):

> a criação de delegacia de polícia especializada em crimes informáticos e inclui na legislação crimes de preconceito de raça ou cor para que a publicação seja interrompida.

Ulteriormente, foi sancionado o Marco Civil da Internet, em 23 de abril de 2014, mesmo ano em que foi revelado o esquema de espionagem do governo norte-americano, no qual foram grampeados 29 telefones de líderes políticos do Brasil (G1, 2015).

A Lei nº 12.965 de 2014 foi essencial para a regulação da utilização da internet no Brasil pela "previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado" (HUDSON, 2014, p. 1).

O texto do Marco Civil da Internet apresenta 32 artigos divididos em cinco capítulos, são eles: (I) apresentação dos princípios e finalidades da utilização da internet no Brasil, (II) identificação dos direitos e garantias dos usuários, (III) fornecimento de conexão de aplicativos no ambiente virtual, (IV) a atuação do Poder Público na regulação da internet e (V) as disposições finais (ANTUNES, 2022, p. 64 e 65). No entanto, não há previsão na lei sobre a responsabilização penal dos agentes envolvidos nas más condutas.

2.2. Aplicação da Convenção de Budapeste no combate aos crimes digitais no Brasil

Consoante exposto anteriormente, a Convenção sobre Crimes Cibernéticos tipificou dez condutas diferentes como criminosas, que devem ser observadas pelos países signatários (DUARTE, 2022, p. 22).

Um dos pontos positivos da adesão do Brasil a esse tratado internacional é sua compatibilidade com as normas internas, consoante demonstrado pelo Conselho Europeu, em tabela elaborada em 2020:

Tabela 1: Correlação entre a Convenção de Cibercrimes e a lei penal brasileira.

Prescrições legais sobre a Convenção de Crimes Cibernéticos		**Prescrição penal no direito brasileiro: Código Penal (CP), Lei de Propriedade intelectual de programa de computador (Lei nº 9.609/98), Estatuto da Criança e do Adolescente (ECA), Norma de Interceptação de Comunicações Telefônicas e Informáticas (Lei nº 9.296/96).**	
Artigo 2	**Acesso ilegal.**	Artigo 154-A e 154-B (CP)	É uma invasão de um dispositivo informático (público ou privado).
Artigo 6	**Uso abusivo de dispositivo digital.**		
Artigo 3	**Interceptação ilegal.**	Artigo 10 (Lei nº 9.296/96)	Interceptação sem autorização judicial.
Artigo 4	**Interferências em dados informáticos.**	-	Sem previsão.
Artigo 5	**Interferência em sistemas.**	Artigo 313-B (CP).	Modificação ou alteração ilícita de sistemas de informação.
Artigo 7	**Falsidade informática**	Artigo 297 (CP)	Falsificação de documentos públicos.
		Artigo 298 (CP)	Falsificação de documentos particulares.
		Artigo 298, parágrafo único (CP)	Falsificação de cartões de crédito ou débito
		Artigo 313-A (CP)	Inserção de dados falsos em sistemas de

			informações
Artigo 8	**Fraude Informática**	Artigo 171 (CP)	Estelionato.
		Artigo 155 (CP)	Furto por fraude.
		Artigo 240 (ECA)	É a produção ou reprodução de conteúdo explícito envolvendo crianças ou adolescentes.
		Artigo 241 (ECA)	Oferecer, comercializar, publicar ou distribuir conteúdo explícito envolvendo crianças ou adolescentes.
		Artigo 241-A (ECA)	Oferecer, comercializar, publicar ou distribuir conteúdo explícito envolvendo crianças ou adolescentes, usando computadores ou redes.
		Artigo 241-B (ECA)	Comprar, possuir ou armazenar conteúdo explícito envolvendo crianças ou adolescentes.
		Artigo 241-C (ECA)	Simular a participação de crianças ou adolescentes em conteúdos explícitos.
Artigo 10	**Infrações relacionadas com a violação dos direitos autorais e direitos conexos.**	Artigo 184 (CP). Artigo 2 (Lei nº 9.609/98).	É uma violação de direitos autorais e direitos relacionados.
Artigo 11	**Tentativa e ajuda ou cumplicidade.**	Artigo 14 (CP)	A tentativa de produzir conduta criminosa é punível.

Fonte: DUARTE, 2022, p. 22

Insta destacar que o Brasil não possui, até o momento, uma compatibilidade completa com a Convenção de Budapeste haja vista não ter assinado o protocolo adicional concernente

à criminalização de condutas de racismo e xenofobia utilizando-se de sistemas informáticos (CONSELHO DA EUROPA, 2022).

Não obstante, o ordenamento jurídico brasileiro apresenta normas compatíveis com as previsões normativas de processo penal dispostas no tratado internacional (CONSELHO EUROPEU, 2022), veja-se:

Tabela 2: Leis processuais penais brasileiras que atendem às determinações da Convenção de Cibercrimes.

Prescrição processual penal no direito brasileiro: ● Código de Processo Penal (CPP) ● Marco Civil da Internet (MCI) ● Lei de Organização Criminosa (Lei nº 12.850/2013) ● Norma de Interceptação de Comunicações Telefônicas e Informáticas (Lei nº 9.296/96) ● Resolução 596/2012 da ANATEL	
Artigo 10 (MCI).	Permite que autoridades policiais e Ministério Público solicitem diretamente aos prestadores de serviços a concessão de acesso aos dados de assinantes dos usuários, isso não inclui endereços IP que necessitam de dependam de ordem judicial.
Artigo 10, §3º (MCI).	Prevê que é necessária uma ordem judicial para que os provedores disponibilizem registros de conexão, bem como conteúdo armazenado de comunicações privadas.
Artigo 240 (CPP)	Fala sobre busca e apreensão tradicionais, mas que também são utilizadas para busca e apreensão de dados informáticos armazenados.
Lei 9.296/1996	Regulamenta a interceptação de comunicação, permitindo a interceptação em sistemas telefônicos e de informática no âmbito de investigações criminais. Essa interceptação está condicionada por ordem judicial e o pedido deve ser justificado por suspeita razoável do crime e pela

	impossibilidade de obtenção de prova por outros meios.
Artigo 10-A (Lei nº 12.850/2013)	Inclui e regulamenta a possibilidade de infiltração virtual de agentes policiais.
Resolução 596/2012 (ANATEL)	Permite que o órgão solicite diretamente às prestadoras de serviços o acesso às informações da conta e aos registros de chamadas dos usuários.
Artigo 10 (MCI).	Permite que autoridades policiais e Ministério Público solicitem diretamente aos prestadores de serviços a concessão de acesso aos dados de assinantes dos usuários, isso não inclui endereços IP que necessitam de dependam de ordem judicial.

Fonte: DUARTE, 2022, p. 24

Para além da compatibilidade entre o tratado internacional e a legislação pátria, a adesão do Brasil à Convenção de Budapeste também representa uma grande mudança do país com relação à cooperação internacional. Considerando que a cooperação jurídica entre nações é uma ferramenta fundamental na repressão dos crimes cibernéticos, esse avanço é positivo para que o Brasil possa tornar mais efetivo o controle de condutas delituosas no meio virtual (VERONESE e CALABRICH, 2022).

Considerações Finais

Apesar de ser um tema discutido desde 1989 em convenções internacionais, a iniciativa brasileira de combater cibercrimes tardou a aparecer e não se mostrou suficiente para responsabilizar os agentes responsáveis pelas más condutas, o que pode ser atestado a partir dos dados apresentados acima sobre o aumento desses crimes no Brasil. Da mesma maneira, ainda que duas leis tenham sido promulgadas nesse sentido em 2014 no país, houve um foco específico e motivado mais pela pressão social do que por uma conscientização geral sobre os perigos envolvendo a utilização do ambiente virtual.

Por outro lado, a Convenção de Budapeste é a norma internacional mais completa, específica e com a maior quantidade de países signatários sobre este tema, de sorte que pode

ser considerada um instrumento eficaz para a investigação e repressão de crimes digitais. Isto posto, a adesão do Brasil a esse tratado revela-se como um progresso na tipificação penal dos delitos cometidos na internet, o que é esperado há algum tempo por diversas autoridades brasileiras.

A Convenção sobre Crimes Cibernéticos é bastante condizente com a base de Direito Penal e Processual Penal brasileira e, por isso, o que poderia representar uma mera adesão a um tratado, em realidade traduz uma solidificação das discussões sobre estes crimes no Brasil. Espera-se que, em breve, o Brasil possa apresentar ainda mais iniciativas para a repressão efetiva dos crimes digitais a fim de acompanhar harmonicamente o progresso mundial no que concerne à regulamentação do ambiente virtual.

Referências bibliográficas

ALVES, Ana Abigail Costa Vasconcelos; MUNIZ, Antônio Walber Matias; CIDRÃO, Taís Vasconcelos. A oportuna e necessária aplicação do direito internacional nos ciberespaços: uma avaliação sobre a convenção de Budapeste. V. 1, 2018.

ALVES, Paulo. Ataque hacker ao STJ: seis coisas que você precisa saber sobre o caso [Online]. Techtudo. 2020. Disponível em: < https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml Acesso em 29 de jan. 2023.

ANTUNES, Priscila Lucas. Da tipificação penal dos ataques cibernéticos no contexto da sociedade de risco: uma abordagem a partir da convenção de Budapeste. *Repositório Institucional da Universidade Federal de Santa Catarina*, 2022. Disponível em: <https://repositorio.ufsc.br/handle/123456789/232487>. Acesso em 19 de jan. 2023.

BRASIL. Constituição da República Federativa do Brasil. 1988.

BRASIL. Decreto nº 7.030/2009. Promulga a Convenção de Viena sobre Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos artigos 25 e 66. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d7030.htm>. Acesso em: 23 de fev. 2023.

CYBERCRIME mobilizes insurance market. *FIDESRJ*, 17 de abr. 2023. Disponível em: <https://fidesrio2023.com.br/en/2023/04/17/cybercrime-mobilizes-insurance-market/#:~:text=The%20technical%20director%20of%20the,where%20there%20were%20187%20billion.>. Acesso em 27 de junho de 2023.

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

BORGES, José Souto Maior. *Curso de Direito Comunitário*. 2. ed. São Paulo: Saraiva, 2009.

CIDRÃO, Taís Vasconcelos; MUNIZ, Antônio Walber; ALVES, Ana Abigail. A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da Convenção de Budapeste à legislação brasileira: The timely and necessary

implementation of International Law in the ciberspace: from the Budapest Convention to Brazilian legislation. *Brazilian Journal of International Relations*, v. 7, n. 1, p. 66-82, 2018.

COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. CRIMINALIDADE DIGITAL NO BRASIL: A PROBLEMÁTICA E A APLICABILIDADE DA CONVENÇÃO DE BUDAPESTE. *Revista Em Tempo*, v. 21, n. 1, p. 104-123, 2021.

COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA, Parecer sobre e o Projeto de Lei da Câmara nº 89, de 2003, e Projetos de Lei do Senado nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática, 2006. Disponível em: <https://www.safernet.org.br/site/sites/default/files/PLS_Azeredo-CCJ-versao-de-19-08-2006.pdf>. Acesso em 5 de mar. 2023.

CONSELHO EUROPEU. Chart of signatures and ratifications of Treaty 185. 16 jun. 2017. Disponível em: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>. Acesso em 21 de jan. 2023.

CONSELHO EUROPEU. Consultations with civil society, data protection authorities and industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime. Estraburgo. Disponível em: <https://www.coe.int/en/web/cybercrime/protocol-consultations> Acesso em 7 de mar. 2023.

CONSELHO EUROPEU. Country Wiki [Online]. Estraburgo. 2021. Disponível em: <https://www.coe.int/en/web/octopus/country-wiki> Acesso em: 7 de mar. 2023.

CONSELHO EUROPEU. Minutes of the Committee PC-CY, 2000 (unpublished)

CONVENÇÃO DE BUDAPESTE. Convenção sobre o Cibercrime. 2001. Disponível, em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf >. Acesso em 17 de jan. 2023.

CSONKA, Peter. The council of europe's convention on cyber-crime and other European initiatives. Revue internationale de droit pénal 2006/3-4 (Vol. 77), p. 473 a 501. Disponível em: <https://doi.org/10.3917/ridp.773.0473>. Acesso em 2 de mar. 2022.

DUARTE, Ana Luísa Vieira. Análise do encaixe da convenção de Budapeste no ordenamento jurídico brasileiro. 2022.

EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeaks. *G1*, 2015. Disponível em: <https://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>. Acesso em 4 de mar. 2023.

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

FLORIANI, Lara Bonemer Rocha; SANTOS, Luccas Farias. A hierarquia dos tratados internacionais e seus reflexos jurídicos e extrajurídicos. *Revista Direitos Sociais e Políticas Públicas–Unifafibe*, v. 7, n. 1, 2019.

GARCIA, Alline Tavares. O DIREITO À INTIMIDADE E A FRÁGIL PRIVACIDADE DA ERA DIGITAL: uma análise sobre os crimes cibernéticos e a eficácia da lei Carolina Dieckmann. 2017.

GARCIA, O.M. La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul cyber-crime. In Il diritto penale dell'informatica nell'epoca di

internet, di L. Picotti. Padova: Cedam, 2004.

GROTTO, Marco. "Council of Europe Convention on cybercrime and its ratification in the Italian legal system." Sistema Penal & Violência 2010.2 (2010): 5.

HENRIK W. K. KASPERSEN, Implementation of Recommendation No R (89) 9 on computer-related crime, Report prepared for the European Committee on Crime Problems, doc. CDPC (97) 5 (não publicado), Strasbourg, 1997, p. 104 a 106).

HUDSON, Alex. O Marco Civil da Internet. Disponível em: <http://rbrj.com.br/tecnologia/>. Acesso em 27 de fev. 2023.

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

LIRA, Leide de Almeida. Lei Carolina Dieckmann: (in) eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos. Conteudo Juridico, Brasilia-DF: 01 jul 2014, 06:45. Disponivel em: <https://conteudojuridico.com.br/consulta/Artigos/40026/lei-carolina-dieckmann-in-eficacia-na-protecao-dos-direitos-fundamentais-a-intimidade-e-a-vida-privada-em-face-da-pena-cominada-aos-delitos-informaticos>. Acesso em 07 de mar. 2023.

MOLITOR, Heloísa Augusta Vieira; VELAZQUEZ, Victor Hugo Tejerina. BREVE PANORAMA SOBRE A LEGISLAÇÃO APLICADA NOS CRIMES ELETRÔNICOS. *Revista de Direito, Governança e Novas Tecnologias*, v. 3, n. 2, p. 81-96, 2017.

NASCIMENTO, Samir de Paula. *Cibercrime:* Conceitos, modalidades e aspectos jurídicos penais. Âmbito Jurídico, 2019. Disponível em: <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitosmodalidades- e-aspectos-juridicos-penais/>. Acesso em: 20 de fev. 2023.

NOTA À IMPRENSA Nº 186. Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública – Adesão do Brasil à Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Disponível em: <https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica-2013-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico-celebrada-em-budapeste-em-23-de-novembro-de-2001>. Acesso em 30 de nov. 2022.

PINHEIRO, Patrícia P. Direito Digital. 2. ed. São Paulo: Saraiva, 2007.

REZEK, José Francisco. Direito Internacional Público: curso elementar. 8. ed. rev. atualizada. São Paulo. Saraiva, 2000.

SENADO FEDERAL. Lei nº 12.737/2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_

ato2011-2014/2012/lei/l12737.htm>. Acesso em: 6 de mar. 2023.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÃO - UIT. Relatório Global de Conectividade 2022. Disponível em: <https://www.itu.int/hub/publication/d-ind-global-01-2022/#> Acesso em 5 de mar. 2023.

VERONESE, Alexandre. CALABRICH, Bruno. Cybercrime in Brazil After the COVID-19 Global Crisis: An Assessment of the Policies Concerning Internacional

Cooperation for Investigations and Prosecutions. 2022. WORLD ECONOMIC FORUM, Global Cyber Security Outlook, 2023. Disponível em: <https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf >. Acesso em 5 de mar. 2023.


OBSERVATÓRIO DA
LGPD
UNIVERSIDADE DE BRASÍLIA