# XII ENCONTRO INTERNACIONAL DO CONPEDI BUENOS AIRES – ARGENTINA

## DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS IV

**DANIELLE JACON AYRES PINTO**

**JOSÉ RENATO GAZIERO CELLA**

**CINTHIA OBLADEN DE ALMENDRA FREITAS**

**PABLO RAFAEL BANCHIO**

D597

Direito, Governança e novas tecnologias IV [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Cinthia Obladen de Almendra Freitas; Danielle Jacon Ayres Pinto; José Renato Gaziero Cella; Pablo Rafael Banchio. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-833-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Derecho, Democracia, Desarrollo y Integración

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XII Encontro Internacional do CONPEDI Buenos Aires – Argentina (2: 2023 : Florianópolis, Brasil).

CDU: 34

CONPEDI

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

# XII ENCONTRO INTERNACIONAL DO CONPEDI BUENOS AIRES – ARGENTINA

## DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS IV

---

## Apresentação

No XII Encontro Internacional do CONPEDI, realizado nos dias 12, 13 e 14 de outubro de 202r, o grupo de trabalho "Direito, Governança e Novas Tecnologias IV", que teve lugar na tarde de 13 de outubro de 2023, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados 11 artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente na Faculdade de Direito da Universidade de Buenos Aires - UBA.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em cinco blocos, quais sejam a) temas de inteligência artificial; b) temas de regulação da internet; c) temas de dados pessoais; d) temas de contratos e blockchain; e e) temas de cidadania, democracia e direitos.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema "Direito, Governança e Novas Tecnologias". Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. José Renato Gaziero Cella

Prof. Dra. Cinthia Obladen de Almendra Freitas

Prof. Dr. Pablo Rafael Banchio

# AVANÇO JURISPRUDENCIAL DA CADEIA DE CUSTÓDIA DE PROVA DIGITAL E A CONVENÇÃO DE BUDAPESTE SOBRE CIBERCRIME

# JURISPRUDENTIAL ADVANCE OF THE CHAIN OF CUSTODY OF DIGITAL EVIDENCE AND THE BUDAPEST CONVENTION ON CYBERCRIME

**Raissa de Cavassin Milanezi** [1]
**Rodrigo Sánchez Rios** [2]
**Cinthia Obladen de Almendra Freitas** [3]

**Resumo**

A prática de crimes informáticos tem sido recorrente nos últimos anos, o que se deve em razão da nova forma de viver e dos sujeitos interagirem socialmente a partir do ambiente digital. O estudo teve por objetivo analisar a cadeia de custódia da prova digital no aspecto doutrinário, jurisprudencial e da Convenção de Budapeste sobre o Cibercrime. Analisa-se a decisão do STJ proferida em RHC n.º 143.169/RJ, de 2023, em que o Tribunal entendeu, em resumo, que a quebra da cadeia de custódia resulta em inadmissibilidade da prova e daquelas que derivam dela. Desta forma, tem-se dois problemas de pesquisa, (i) o de analisar o avanço jurisprudencial no tocante à cadeia de custódia da prova digital e (ii) o de verificar quais foram os impactos com o advento da Convenção de Budapeste na temática em pauta. Utilizou-se método dedutivo, com procedimento teórico e técnica bibliográfica. Conclui-se que a preponderância do STJ em inadmitir provas que não observem os aspectos técnicos para a manutenção da cadeia de custódia, bem como que a Convenção de Budapeste é importante em termos de cooperação internacional, mas ela está afeta ao sistema de garantias constitucionais.

**Palavras-chave:** Provas digitais, Cadeia de custódia da prova digital, Crimes informáticos, Ciberespaço, Sociedade informacional

**Abstract/Resumen/Résumé**

The practice of cybercrime has been recurring in recente years, which is due to the new way of living and the subjects interacting socially from the digital environment. The objective of the study was to analyze the chain of custody of digital evidence from a doctrinal, jurisprudential, and Budapest Convention on Cybercrime perspective. The decision of the

[1] Mestranda em Direito Econômico e Desenvolvimento da PUCPR. Pós-graduada em Ciências Criminais e em Direito, Tecnologia e Inovação: Proteção de Dados. Professora de Processo Penal. E-mail: raissadcm@gmail.com

[2] Doutor em Direito pela Università degli studi di Roma III - La Sapienza. Professor de Direito penal da PUCPR. Advogado criminalista.

[3] Doutora em Informática. Professora Titular e Coordenadora do Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Membro da Comissão de Direito Digital e Proteção de Dados da OAB/PR. E-mail: cinthia.freitas@pucpr.br

STJ (Superior Court of Justice) in RHC n.º 143.169/RJ, 2023, was analyzed, where the Court understood that the breach of the chain of custody results in the inadmissibility of the evidence and its derived evidence. Therefore, two research problems arise: (i) analyzing the jurisprudential progress regarding the chain of custody of digital evidence, and (ii) examining the impacts with the advent of the Budapest Convention on the subject matter. A deductive method was used, with theoretical procedure and bibliographic technique. It is concluded that the STJ predominance in rejecting evidence that does not comply with technical aspects for maintaining the chain of custody, as well as the importance of the Budapest Convention in terms of international cooperation, while being subject to constitutional guarantees of the Brazilian system.

**Keywords/Palabras-claves/Mots-clés:** Digital evidence, Chain of evidence of digital evidence, Cybercrimes, Cyberspace, Information society

## 1. INTRODUÇÃO

O Pacote Anticrime trouxe avanços no tocante ao registro do procedimento da cadeia de custódia da prova em âmbito processual penal. Entretanto, em que pese a Lei n.º 13.964/2019 (BRASIL, 2019) tenha inaugurado a diretriz procedimental da cadeia de custódia, antes dela o Código de Processo Penal, em seu artigo 158, já dispunha sobre a necessidade de registro probatório, ainda que se referindo ao exame de corpo de delito.

De igual forma, a doutrina já vinha se manifestando sobre a temática à luz do princípio do contraditório e da ampla defesa, na medida em que o registro da cadeia de custódia é salutar para dar efetividade aos direitos constitucionais do acusado.

Na definição de Geraldo Prado, "a cadeia de custódia da prova nada mais é que um dispositivo dirigido para assegurar a fiabilidade do elemento probatório, ao colocá-lo sob proteção de interferências capazes de falsificar o resultado da atividade probatória." (PRADO, 2019, p. 50).

Todavia, com a aprovação do Pacote Anticrime e com o avanço de crimes cometidos em ambiente informático, a temática da manutenção da cadeia de custódia está cada vez mais presente na jurisprudência e na doutrina.

Em razão de tal contexto é que se extrai a importância do artigo, na medida em que o Brasil é alvo constante de ataques cibernéticos (JORNAL DA USP, 2023), ataques que além de ofenderem de forma individual, trazem contornos para a economia e para própria democracia.

Desta forma, o artigo tem por objetivo responder a 02 (dois) problemas de pesquisa, quais sejam, (i) o de analisar o avanço jurisprudencial no tocante à cadeia de custódia da prova digital e o (ii) de verificar quais foram os impactos com o advento da Convenção de Budapeste na temática em pauta.

No tocante ao procedimento metodológico, a pesquisa utilizou do método dedutivo, com procedimento teórico e técnica bibliográfica. Inicia-se apresentando aspectos gerais do Direito Informático em razão dos novos contornos dados no ciberespaço, haja vista que essa nova forma de viver engendrada pela sociedade informacional passou a refletir na interação dos sujeitos como um todo (CASTELLS, 2003), inclusive da criminalidade, eis que o modelo de capitalismo é forjado por uma economia informacional, global e em rede (CASTELLS, 2022). Segue-se analisando alguns julgados proferidos pelo STJ que envolvem a temática da cadeia de custódia em

paralelo com o que a doutrina expõe sobre o tema, de forma a dar ênfase no julgamento do Habeas Corpus n.º 133.440, em que o STJ considerou como inadmissível uma prova obtida em inobservância ao regramento da cadeia de custódia.

Dessa forma, discute-se os aspectos da Convenção de Budapeste (Convenção de Cibercrime), recentemente incorporada ao ordenamento jurídico brasileiro, de forma a apontar se a legislação impactou na procedimentalidade da cadeia de custódia dos crimes informáticos. Ao final, observou-se que o julgamento do RHC n.º 143.169, do Rio de Janeiro, foi de extrema importância, tendo em vista que assentou o entendimento do STJ sobre a obrigatoriedade da cadeia de custódia dos crimes informáticos, bem como que a Convenção de Budapeste constitui um instrumento importante de cooperação internacional, que deve ser alinhado com o aspecto de última razão do Direito Penal e com políticas públicas efetivas para solução do problema público.

O artigo é resultado de projeto de pesquisa financiado pelo Programa de Cooperação Acadêmica em Segurança Pública e Ciências Forenses (PROCAD/SPCF) da Coordenação de Aperfeiçoamento de Pessoal em Nível Superior (CAPES).

## 2. SOCIEDADE INFORMACIONAL: CONTORNOS DADOS NO CIBERESPAÇO

A sociedade é influenciada pelas tecnologias da informação e da comunicação (TICS), o que fez e faz com que a criminalidade também migrasse para um novo espaço: o virtual. Esse rearranjo, se deve ao advento massivo da internet, em que a sociedade contemporânea passou a se organizar socialmente em redes online, alterando significativamente a economia e a cultura, que agora é globalizada e ávida por compartilhamento e dados (CASTELLS, 2003).

A sociedade de risco, explicitada por Beck, rememora o quanto o corpo social é refém da exploração humana, que foi intensificada com a revolução industrial e que é marcada por um risco constante e compartilhado, sendo esse risco forjado pela passagem da era moderna para a pós-moderna (BECK, 2011, p. 7-30).

Já a sociedade informacional, segundo Castells, é marcada pelo uso constante de ferramentas tecnológicas, o que faz com que a tecnologia seja a própria sociedade (CASTELLS, 2022). Segundo Boff, Fortes e Freitas, a sociedade da informação é marcada por uma "*forma específica de organização social na qual a geração, o processamento e a transmissão de informação se convertem nas fontes fundamentais da*

*produtividade e do poder por conta das novas tecnologias."* (BOFF, FORTES e FREITAS, 2018, p. 9).

A sociedade de risco e a informacional se interrelacionam, já que os riscos advindos das tecnologias também são desconhecidos e, por vezes, imperceptíveis, a exemplo dos reflexos destacados por Shoshana Zuboff ao explicar a era do capitalismo de vigilância (ZUBOFF, 2020).

Segundo Spencer Sydow, ao mesmo tempo em que a modernização traz vantagens aparentes na maximização de valores, ela também traz outro reflexo, que é o descontrole da harmonia social (SYDOW, 2022, p. 38). A sociedade da informação, portanto, "*teve sua potência elevada com a popularização das máquinas e suas conexões, bem como com a chegada dos smartphones, levando à boa parte da população o acesso a um cotidiano com características próprias (...)"* (SYDOW, 2022, p. 39), ferramentas que foram rapidamente aceitas pela população, mas que ao mesmo tempo expõem todo corpo social a riscos que são desconhecidos.

Conforme exposto por Sydow, a internet constitui uma parcela da virtualidade em que os sujeitos se relacionam de forma ampla, na medida em que constroem sua reputação, se movimentam financeiramente e utilizam o espaço para diversas outras relações, tais como, trabalho e entretenimento, ao passo em que fornecem seus dados com a expectativa de que determinado dispositivo informático oferecerá segurança (SYDOW, 2022, p. 43).

Contudo, sabe-se que esse ambiente também está sujeito a riscos, que são designados por Sydow como riscos informáticos. Segundo este autor, os riscos informáticos são aqueles que colocam em risco bens jurídicos informáticos ou bem jurídicos comuns, a exemplo, *"*a *tranquilidade para navegar, a segurança para se fazer operações em plataformas digitais, o acesso à virtualidade propriamente dito, a integridade dos arquivos armazenados, a confiabilidade da nuvem, a não destruição da imagem virtual construída*" e outros (SYDOW, 2022, p. 43).

No entanto, é preciso rememorar que o Código de Processo Penal é de 1941, ao passo em que o Código Penal é de 1940. Em razão disso, face a migração dos sujeitos para o ciberespaço, é que diversas legislações foram editadas nos últimos anos na tentativa de resolver os problemas sociais de uma sociedade que é marcada pela fluidez, interconexão e velocidade (CASTELLS, 1999, p. 422-499) e que utiliza do direito penal como instrumento para controle social (BATISTA, 2007, p. 65).

Dentre tais legislações, tem-se, por exemplo, a Lei n.º 12.737/2012, que dispõe sobre a tipificação de crimes informáticos e dá outras providências, bem como diversas alterações legislativas no próprio Código Penal que promoveram, por exemplo, a inclusão do crime de invasão informática (artigo 154-A e 154-B, CP) e de divulgação de cena de estupro ou cena de estupro de vulnerável, de cena de sexo e pornografia (artigo 218-C, CP).

Todavia, faz-se importante destacar que, mesmo com a existência de novas legislações para tipificação de crimes cometidos através dos instrumentos advindos com a Tecnologia da Informação e Comunicação (TIC), alguns crimes que antes eram cometidos em meio comum, passaram a ser perpetrados também pelos aludidos meios tecnológicos. Crimes esses que no campo dogmático são designados como crimes impróprios, a respeito do tema:

> (a) Nos crimes informáticos impróprios, os meios digitais são usados como instrumento delitivo. O fim de proteção da norma não é a inviolabilidade da informação automatizada de dados, mas bens jurídicos diversos e, corriqueiramente, tradicionais. (GURAGNI, RIOS, 2019, p. 176).

Assim, tem-se a relevância do Direito Penal Informático, que constitui um ramo importante para o estudo dos crimes cometidos no ciberespaço, especialmente frente a tecnicidade exigida no processo persecutório, que é incomum ao operador do Direito, que agora precisa aprimorar seu tecnicismo para além do conceito de crime – conduta típica, antijurídica e culpável.

A exemplo, o operador do Direito que atua com a persecução de crimes informáticos, deve compreender o que são os ataques de *ransonware*, atividades com *malware*, *crytojacking*, ciberextorção, incitação, produção ou posse de pornografia infantil (KASPERSKY, 2023) para conseguir valorar se determinada conduta se amolda ao verbo nuclear de determinado tipo penal, em homenagem ao princípio da reserva legal e da taxatividade.

Um dos grandes problemas disso, é a assimetria informacional, que já é típica no Direito Penal e que se agrava para a persecução dos crimes informáticos, especialmente dos crimes informáticos próprios, já que a assimetria pode ocorrer tanto em relação a (i) seleção/omissão de provas por parte da acusação, quanto em face do (ii) próprio operador do Direito, que por vezes, não tem aptidão técnica para análise de determinado conteúdo probatório.

Acerca da análise do conteúdo probatório, oportuno destacar que, em que pese a Ordem dos Advogados do Brasil tenha regulamentado o procedimento n.º 188/2018 (OAB, 2018), que dispõe sobre a investigação criminal defensiva, é certo que acusados hipossuficientes, sejam eles representados pela Defensoria Pública ou por advogados dativos, sequer conseguem, por vezes, diminuir a aludida assimetria informacional, já que o Estado não dispõe de recursos específicos para contratação de assistentes técnicos, por exemplo.

Como destacado por Caio Badaró Massena (MASSENA, 2023, 3), o Ministério Público, por vezes, fragmenta os procedimentos investigatórios, o que resulta em quebra da unidade processual, sendo que disso também se extrai a importância da cadeia de custódia da prova, que é justamente uma das tentativas de diminuir a assimetria informacional existente entre o Estado e o acusado.

## 3. CADEIA DE CUSTÓDIA DE PROVA DIGITAL: UM PARALELO ENTRE A DOUTRINA E A JURISPRUDÊNCIA

A cadeia de custódia de prova com a descrição de sua procedimentalidade foi incorporada na legislação processual penal por intermédio do Pacote Anticrime, que inseriu os artigos 158-A, B, C, D, E e F, estabelecendo que a cadeia de custódia constitui o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

De acordo com Geraldo Prado, a cadeia de custódia da prova é necessária, tendo em vista que a ausência dela pode conduzir a uma investigação incontrolável e meramente retórica (PRADO, 2019, p. 118).

Para (LOPES JÚNIOR, 2020, p. 725), a cadeia de custódia constitui condição para validade da prova em âmbito processual penal. No entanto, ainda segundo o mesmo autor, antes mesmo das inclusões feitas com o Pacote Anticrime, a doutrina e a jurisprudência já vinham se debruçando sobre a necessidade de unicidade da cadeia de custódia, a exemplo de um habeas corpus julgado no ano de 2014 (HC n.º 160.662), em que o STF entendeu pela ilicitude de uma interceptação telemática justamente em razão da perda de sua unidade, o que, segundo a Corte, acabou prejudicando a integralidade da prova e o exercício da ampla defesa.

Assim, é de se notar que antes mesmo da aprovação do Pacote Anticrime, a temática aqui analisada já havia sido questionada na prática forense, ganhando, evidentemente, mais destaque após a aprovação do Pacote Anticrime.

De forma cronológica, destaca-se dois julgados importantes, o primeiro é do ano de 2021, em que o STJ debateu duas correntes que envolviam a quebra da cadeia de custódia (*break in the chain of custody*). Em síntese, tais correntes entendiam que, (i) a quebra da cadeia de custódia ocasiona a ilicitude da prova e daquelas por derivação, resultando na necessidade de exclusão dos autos; (ii) que a quebra da cadeia de custódia não levaria, de forma obrigatória, à ilicitude da prova, devendo o Magistrado sopesá-las de acordo com todos os elementos produzidos na instrução. A corrente descrita no item (ii) foi a que prevaleceu à época, conforme entendimento do STJ no HC 653.515/RJ, que levou em consideração as especificidades do caso concreto, ponderando, ainda, que o legislador se quedou "*silente em relação aos critérios objetivos para definir quando ocorre a quebra da cadeia de custódia e quais as consequências jurídicas, para o processo penal, dessa quebra ou do descumprimento*" (STJ, HC 653.515/RJ).

No entanto, mais recentemente, em janeiro de 2023, o STJ assentou-se na necessidade da manutenção da cadeia de custódia. A Corte, em sede de recurso em habeas corpus (STJ, HC 143.169/RJ), entendeu que (i) a falta de documentação no tratamento de provas afeta a confiabilidade dela; (ii) tendo por consequência a inadmissão da prova, (iii) que a manutenção da cadeia de custódia é de ônus do Estado, não tendo aplicação a presunção de veracidade quando descumpridos os procedimentos da temática de estilo, bem como (iv) que, em que pese a legislação prevista no Pacote Anticrime não retroaja, a necessidade da manutenção da cadeia de custódia não surgiu com o conjunto de alterações legislativas, já que tal requisito de integralidade da prova estava ligada com o conceito de corpo de delito, nos termos do artigo 158, do CPP, de forma que o registro sequencial da prova é necessário até mesmo para os fatos que ocorreram antes de 2019 (após a aprovação do Pacote Anticrime).

O julgado destacado acima, registrado sob número 143.169, do Rio de Janeiro, de relatoria do Ministro Messod Azulay Neto, é de extrema importância, principalmente no que se refere aos crimes informáticos, eis que o STJ destacou a necessidade de armazenamento integral do conteúdo do dispositivo periciado, de forma a gerar um arquivo que espelha e representa de forma fiel o conteúdo original.

Ainda, o STJ destacou que, por meio da técnica denominada *hash*, "*é possível obter uma assinatura única para cada arquivo, que teria um valor diferente caso um*

*único bit de informação fosse alterado em etapa da investigação, quando a fonte de prova já estivesse sob custódia da polícia*.” (STJ, RHC 143.169). A técnica do algoritmo *hash* é de extrema importância, porque ela garante a “*autenticidade, a integridade, confiabilidade e a veracidade do material criptografado*” (FREITAS, PIRATELLI e SOUSA, 2022, p. 37)., de modo que “*eventual alteração na prova digital ocasionará alteração do próprio hash, cuja ausência de correspondência com o hash original demonstra que a cadeia de custódia foi violada*.” (FREITAS, PIRATELLI e SOUSA, 2022, 37). Há que se esclarecer que o *hash* é resultado da aplicação de técnicas de criptografia em conteúdos digitais.

A aludida técnica descrita por Freitas, Piratelli e Souza consta também na ementa do RHC 143.169, confira-se:

> 4. A autoridade policial responsável pela apreensão de um computador (ou outro dispositivo de armazenamento de informações digitais) deve copiar integralmente (bit a bit) o conteúdo do dispositivo, gerando uma imagem dos dados: um arquivo que espelha e representa fielmente o conteúdo original. 5. Aplicando-se uma técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo, que teria um valor diferente caso um único bit de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Comparando as hashes calculadas nos momentos da coleta e da perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi modificado. (STJ, RHC 146.139, 2023)

Na eventualidade da cadeia de custódia não ser preservada – sendo “*ônus do Estado comprovar a integridade e confiabilidade das fontes por ele apresentadas*” (STJ, RHC 143.169, 2023) - os elementos probatórios do vestígio não podem ser aproveitados (MATIDA, 2020), não sendo admitido ao Estado agir de forma irregular e tampouco é cabível a simples alegação de presunção de veracidade das alegações estatais quando o regramento do artigo 158-A e seguintes do Código de Processo Penal forem desrespeitados (STJ, RHC 146.169, 2023).

Desta feita, observa-se o avanço jurisprudencial sob a ótica de uma concepção garantista no tocante a preservação da cadeia de custódia, homenageando assim, a legislação processual penal e a Constituição Federal, que tem por primado a ampla defesa e o contraditório.

Entretanto, tem-se como necessário registrar que existem diversos outros julgados em sentido contrário ao destacado acima, mas o RHC n.º 143.169 ganhou destaque justamente por enfrentar questões que envolvem a cadeia de custódia da prova digital.

## 4. A CONVENÇÃO DE BUDAPESTE SOBRE CIBERCRIME: IMPACTOS NA CADEIA DE CUSTÓDIA

A Convenção de Budapeste sobre Cibercrime foi incorporada no ordenamento jurídico por intermédio do Decreto Lei n.º 11.491/2023 e dispõe sobre normas de Direito Penal material e Direito Processual Penal, tendo por principal objetivo a cooperação entre os Estados e Partes.

De acordo com o Ministério das Relações Exteriores, a adesão do Brasil à Convenção agilizará o trabalho das autoridades brasileiras e tem outros 67 países aderentes, a exemplo, do Chile, Argentina e República Dominicana (CÂMARA DOS DEPUTADOS, 2021).

A Convenção Internacional sobre Cibercrime foi desenvolvida pelo Conselho da Europa e é "*considerada como a norma internacional mais completa que até hoje existe, uma vez que fornece uma estrutura abrangente e coerente sobre cibercrime e prova eletrônica.*" (CONSELHO DA EUROPA, 2019), constituindo, ainda de acordo com o Conselho, um marco importante para um país que pretenda combater o cibercrime com estrutura internacional dos países aderentes.

De acordo com Waldman e Coltro, em artigo publicado antes da promulgação da Convenção, o Brasil estava defasado no tocante à tutela de condutas praticadas pelos meios digitais, o que resultava em uma verdadeira ineficiência do *jus puniendi* em relação aos crimes virtuais (WADMAN E COLTRO, p. 7).

Barboza destaca que a criminalidade cibernética possui caráter transnacional, não se limitando a extensão territorial de um Estado, o que fomenta a necessidade de uma política informacional voltada a cooperação internacional (BARBOZA, 2023, p. 84), de tal forma que a Convenção de Budapeste contempla tal necessidade.

Para Alves, Muniz e Cidrão, a Convenção é um instrumento eficaz, haja vista que uniformiza o direito material e processual penal, contudo, deixa falhas "*quando obriga o país signatário menos desenvolvido a adotar às mesmas adequações legais dos países mais desenvolvidos, sem a observância do grau da evolução tecnológica, da capacitação humana e recursos tecnológicos que cada estado membro possui.*" (ALVES, MUNIZ, CIDRÃO, 2023, p. 10).

Para Figueiredo e Rios, a adesão do Brasil à Convenção de Budapeste "*inaugura um marco legislativo capaz de compor a demanda nacional de cooperação internacional*

*no combate à cibercriminalidade, a fim de controlar a cooperação entre Estados em face da realidade tecnológica (...)".* (FIGUEIREDO, RIOS, 2023, p. 13).

Jesus e Milagre apontam que a Convenção de Budapeste tem por finalidade a de estabelecer diretrizes às políticas nacionais para o enfrentamento dos crimes cibernéticos (JESUS, MILAGRE, 2016, p. 53-55).

De acordo com uma nota expedida pela Associação Brasileira de Internet, a Convenção é importante, eis que o Brasil passa a fazer parte de uma rede internacional de cooperação que atuará em 24 horas diárias, justamente para responder os pedidos de assistência e acesso a provas eletrônicas envolvendo infrações penais (ASSOCIAÇÃO BRASILEIRA DE INTERNET, 2023), tal qual como prevê o artigo 35 da Convenção de Budapeste - Sistema de Plantão 24 por 7.

Para o Conselho da Europa, órgão responsável pela elaboração da Convenção, os países que aderirem e aderissem ao documento contariam e contam com alguns benefícios descritos pelo próprio Conselho, a exemplo de programas de capacitação, de possibilidade de participação em negociações futuras, bem como de maior cooperação do setor privado, haja vista que, os indicadores do ente demonstram a tendência do setor privado de cooperação com os Estados membros da Convenção (CONSELHO DA EUROPA, 2019).

Oportuno destacar que a Convenção sobre Cibercrime surgiu mediante a demanda, sobretudo dos países europeus, em relação a necessidade de unicidade internacional para cooperação de crimes que têm como características a mobilidade, conversabilidade, conectividade, mundialização, ubiquidade ou simultaneidade e especialmente de não territorialidade (SYDOW, 2022, p. 281-308).

Assim, o próprio preâmbulo do Decreto n.º 11.491, de 12 de abril de 2023, dá conta justamente disso, ao dispor que um dos principais objetivos do documento é a cooperação internacional dos Estados membros do Conselho da Europa e das demais Partes de atuar no combate à criminalidade de forma mais intensa, rápida e eficaz, bem da ciência dos signatários adotarem "*uma política criminal comum destinada à proteção da sociedade contra o crime cibernético, nomeadamente pela adoção de legislação apropriada e pela promoção da cooperação internacional, entre outras medidas*." (CONSELHO DA EUROPA, 2019).

No aspecto estrutural, como já exposto, a Convenção prevê diretrizes de Direito Penal e de Direito Processual Penal, inclusive com aspectos que envolvem o Direito Internacional. Possivelmente em razão da tecnicidade do ciberespaço, a Convenção

promoveu, já no capítulo I, a definição de questões terminológicas, explicitando o que se considera, para fins da Convenção, sistema de computador, dados de computador, provedor de serviço e dados de tráfego.

Em linhas gerais, a Convenção possui quatro capítulos; Terminologia, Medidas a Tomar em nível Nacional, Cooperação Internacional e Disposição finais, estrutura que se divide em 48 artigos. No entanto, ao contrário do que é corriqueiramente noticiado nas mídias, o instrumento legal não criou tipos penais, apenas considerou que "*cada parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna"* (BRASIL, 2023) condutas que envolvem, por exemplo, falsificação informática, fraude informática, pornografia infantil, violação de direitos autorais e de direitos correlatos e outros crimes.

Além disso, a Convenção de Cibercrime também estipulou a responsabilidade penal da pessoa jurídica (artigo 12), dispondo que cada parte adotará medidas legislativas necessárias para assegurar que pessoas jurídicas possam ser consideradas penalmente responsáveis por crimes tipificados de acordo com a Convenção. Santos aponta que tal preocupação de responsabilização da pessoa jurídica teve como origem um processo judicial na Alemanha, em face da empresa Compuserve, no ano de 1997 (SANTOS, p. 13):

> De outra banda, na Europa, a preocupação com a responsabilização da pessoa jurídica, no campo da delituosidade informática, ocorreu após o processo judicial, na Alemanha, em face da empresa Compuserve, em 1997. O provedor foi condenado, em primeira instância, por difundir material pornográfico infantil, advindo dos Estados Unidos; sublinhe-se, porém, que tal decisão foi reformada no tribunal germânico. De toda forma, a doutrina alemã ressaltou a atipicidade da responsabilidade do provedor. A solução foi a implementação de reformas legislativas, tanto em nível estadual quanto federal, a partir de agosto de 1997. Entretanto, as reformas referidas são limitadas, ou seja, implicam o conhecimento do conteúdo proibido por parte dos provedores, a respectiva omissão na prevenção e na circulação e seu subsequente bloqueio. (SANTOS, p. 13).

Todavia, sabe-se que a responsabilização da pessoa jurídica não constitui matéria afeta ao legislador infraconstitucional. Além disso, ainda em matéria penal, o documento prevê que cada Parte deve adotar medidas eficazes, adequadas e dissuasivas, que incluam a privação de liberdade no tocante a tipificação dos crimes previstos na Convenção de Cibercrime.

Feitas tais considerações e tendo em vista que o objetivo do artigo é o de analisar os possíveis impactos da Convenção de Budapeste na temática da cadeia de custódia, tem-

se como destaque o contido no artigo 14, da Seção 2, que é justamente a seção que inaugura a matéria de Direito Processual Penal. De acordo com a Convenção de Cibercrime, "*cada parte adotará medidas legislativas e outras providências necessárias para estabelecer os poderes e procedimentos previstos nesta seção para o fim específico de promover investigações ou processos criminais.*" (BRASIL, 2023).

Diante disso, é que a Convenção prevê a assistência mútua em relação a medidas cautelares, em que (i) qualquer parte pode pedir a outra a conservação de dados armazenados em um computador, localizado no território de outra parte (artigo 29) ou auxílio quando (ii) for necessário a revelação de dados de tráfego para identificação do provedor de serviços que está em outro Estado (artigo 30).

Além disso, os Estados e Partes participantes da Convenção adotam um modelo de assistência mútua em relação a poderes investigativos, em que qualquer Parte pode pedir a outra que realize a busca, acesso, apreensão, guarda ou revelação de dados armazenados por meio de um sistema de computador localizado no território da Parte requerida (artigo 31); solicitação de interceptação de dados de tráfego em tempo real (artigo 33) e requerimento de assistência mútua em relação à interceptação do conteúdo de comunicações específicas transmitidas por meio de um sistema de computador (artigo 34).

Quando os dados de computador disponíveis ao público forem de fonte aberta, independentemente de onde os dados estejam geograficamente localizados uma Parte poderá, sem a autorização da outra, agir. De igual forma, se a parte obtiver o legítimo e voluntário consentimento de uma pessoa que tenha autoridade legal para revelar os dados à parte interessada, o Estado parte pode acessar ou receber, por meio de um sistema de computador em seu território, os dados de computador armazenados no território de outra Parte (BRASIL, 2023).

No Brasil, o órgão competente para análise das funções é o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça e Segurança Pública (GOV, 2023).

De acordo com Murata e Torres, os novos instrumentos adotados pela Convenção de Budapeste têm por finalidade o de agilizar e tornar mais eficiente a obtenção de provas, no entanto, a efetividade depende "*da adoção de medidas para regulamentar o rito cooperacional, permitindo a participação e o controle pelos indivíduos envolvidos e afetados pelos atos cooperacionais.*" (MURATA, TORRES, 2023, p. 1-4).

É certo que os novos instrumentos advindos com a adesão do Brasil à Convenção já impactaram o cenário brasileiro, a exemplo de uma decisão recente do Supremo Tribunal Federal, divulgada no Informativo n.º 1084, ADC 51/DF, Relatoria do Ministro Gilmar Mendes, que antes do Decreto n.º 11.491/2023, entendeu pela admissibilidade das autoridades nacionais requisitarem dados diretamente a provedores no exterior, face ao contido no artigo 11 do Marco Civil da Internet e do artigo 18 da Convenção de Budapeste.

Na prática, de acordo com o julgado destacado acima, as empresas de tecnologia que operam aplicações de internet em território brasileiro devem cumprir determinações do Poder Judiciário brasileiro quando determinado o fornecimento de dados em prol de investigações criminais, mesmo quando os dados estiverem localizados em países estrangeiros.

Desta forma, observa-se que a Convenção é importante em termos de cooperação internacional, entretanto, determinada prova somente pode ser utilizada e colhida se a regra procedimental da cadeia de custódia for observada, mormente ao status constitucional da norma que prima pelo contraditório e ampla defesa. Além do mais, como exposto anteriormente, a Convenção prevê que cada parte deve adotar medidas legislativas e outras providências necessárias para os procedimentos previstos na seção que trata das investigações criminais (Seção 2), o que deve ser interpretado como uma observância a todos os regramentos dispostos na legislação brasileira.

A Convenção está afeta ao sistema de garantias constitucionais e aos instrumentos de Direitos Humanas, assim, ainda que a Convenção não trate de forma específica acerca da cadeia de custódia, isso não retira a submissão dela a norma cogente disposta no artigo 158, do Código de Processo Penal, até mesmo porque a própria Convenção de Cibercrime anuncia que ela está sujeita a tratados internacionais.

No mais, o artigo 19º, ao tratar da proteção de dados de computadores acessados, dispõe que as partes devem adotar uma série de medidas:

> a. apreender ou proteger um sistema de computador ou parte dele ou um meio de armazenamento de dados;
> b. fazer e guardar uma cópia desses dados de computador;
> c. manter a integridade dos dados de computador relevantes;
> d. tornar inacessíveis esses dados no sistema de computador acessado ou dele removê-los. (BRASIL, 2023)

Essa série de medidas, se observadas corretamente e em conjunto com a técnica forense adequada, garantirão a "*autenticidade, a integridade, confiabilidade e a veracidade do material*" (FREITAS, PIRATELLI e SOUSA, 2022, p. 37). Porém, para a preservação da cadeia de custódia é necessário que o material apreendido em proveito de determinada persecução penal seja (i) copiado *bit-a-bit*, garantindo a preservação e o acesso aos dados em caso de falha daquela mídia (CARNEIRO, 2017, p. 44); (ii) após, a prova deve receber a técnica *hash*, "*que é um algoritmo único que mapeia dados e gera um padrão capaz de identificar o arquivo (no caso, a cópia)*" – gerando uma identificação única para o arquivo digital e é por intermédio do número *hash* que a integridade da prova será verificada (SYDOW, 2022, p. 206-207). A procedimento de cópia bit-a-bit é denominado de espelhamento de mídia (CARNEIRO, 2017, p. 44).

Deste modo, observa-se que se tão somente for realizada a cópia do material apreendido, sem a devida cautela da perícia forense, a cadeia de custódia não será preservada, já que a regra procedimental do processo penal deve ser seguida à risca, justamente porque a formalidade é também uma garantia (LOPES JÚNIOR, 2020).

## 5. CONCLUSÃO

A Convenção de Budapeste constitui um instrumento importante em termos de cooperação internacional para o fortalecimento dos países no combate aos crimes informáticos. Entretanto, é preciso registrar que alguns dispositivos foram incorporados de forma acrítica, a exemplo da punição das pessoas jurídicas, que possui restrição no ordenamento jurídico brasileiro.

A Convenção dá primazia a utilização do Direito Penal como instrumento de combate ao Cibercrime, no entanto, tem-se como necessário destacar que o Direto Penal sempre deve observar o caráter de última razão, de tal forma que o combate ao crime envolvendo delitos informáticos deve primar por políticas públicas efetivas.

De igual forma, ainda que a Convenção tenha sido adotada pelo Brasil, ela está afeta ao sistema de garantias constitucionais e aos direitos humanos e fundamentais, sendo a última espécie de direito foi inclusive destacada no preâmbulo da Convenção de Cibercrime, que enumera que os aderentes devem assegurar o devido equilíbrio entre os interesses dos órgãos de persecução criminal e aos direitos humanos fundamentais, observando os tratados internacionais de estilo.

Assim, observa-se que a Lei n.º 11.491/2023 constitui um marco importante para harmonia normativa em nível internacional. No entanto, a persecução penal deve observar os regramentos infraconstitucionais, constitucionais, que são de caráter cogente e a técnica de perícia forense adequada, sob pena de invalidade da prova. Eis aqui o momento que os aspectos jurídicos e tecnológicos caminham lado a lado para garantir provas digitais e sua correta admissibilidade em processos judiciais.

Observou-se que a cópia da prova *bit-a-bit* aliada com a técnica do algoritmo *hash* garantem a cadeia de custódia da prova e são de extrema importância para verificar se o registro sequencial do material periciado foi alterado.

No campo jurisprudencial, evidenciou-se o avanço do STJ em reconhecer a necessidade de manutenção da cadeia de custódia dos crimes informáticos, primando, portanto, pela aplicação dos princípios do contraditório e da ampla defesa, já que somente com o registro sequencial de uma prova utilizada em proveito de uma persecução é que se provê a efetividade do sistema de garantias constitucionais.

## REFERÊNCIAS


ALVES, Ana Abigail Costa Vasconcelos; MUNIZ, Antônio Walber Matias; CIDRÃO, Vasconcelos Taís. A oportuna e necessária aplicação do direito internacional nos ciberespaços: uma avaliação sobre a Convenção de Budapeste. Revista Direito e Liberdade, v. 2, n. 1, 2023.

Associação Brasileira de Internet. **Brasil adere à Convenção de Budapeste sobre Cibercrime.** Disponível em: https://www.abranet.org.br/Noticias/Brasil-adere-a-Convencao-de-Budapeste-sobre-cibercrime-4294.html?UserActiveTemplate=site&UserActiveTemplate=mobile. Acesso em: 02 ago. 2023.

BARBOSA, Hugo Leonardo. **O reconhecimento mútuo do direito à proteção de dados pessoais pelo Brasil e pela União Europeia como forma de concretizar o acesso transfronteiriço a dados informáticos armazenados para o enfrentamento do cibercrime**. Dissertação (Programa de Pós-Graduação em Direito) - Universidade Federal de Santa Catarina, Florianópolis, 2023. 145 f.

BATISTA, NILO. **Introdução crítica ao direito penal brasileiro.** 11. ed. Rio de Janeiro: Revan, 2007.

BECK, Ulrich. **Sociedade de risco:** rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011. p. 7-30.

BOFF, Oro Salete; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de Dados e Privacidade:** Do Direito às Novas Tecnologias na sociedade da Informação. Rio de Janeiro: Lumen Juris, 2018.

BRASIL. Decreto n. 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Diário Oficial da União, Brasília, DF, 12 abril 2023.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Altera a legislação penal e processual penal. Diário Oficial da União, Brasília, DF, 26 dez. 2019. Seção 1, p.1.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Dispõe sobre crimes cometidos por meio da internet. Diário Oficial da União, Brasília, DF, 28 maio 2021. Disponível em: <link>. Acesso em: 01 ago. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. Convenção de Budapeste é promulgada no Brasil. Diário Oficial da União, Brasília, DF, 12 abr. 2023. Seção 1, p. 1.

BRASIL. Superior Tribunal de Justiça. AGRG no HC 143.169/RJ, Relator Ministro Jesuíno Rissato.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus 160.662/RJ, Relator Ministra Assusete Magalhães.

BRASIL. Superior Tribunal de Justiça. HC 653.515/RJ, Relatora Ministra Laurita Vaz.

BRASIL. Superior Tribunal de Justiça. RHC 143.169/RJ. Relator Ministro Messod Azulay Neto, 5ª. Turma.

BRASIL. Ordem dos Advogados do Brasil. Provimento n. 188/2018.

CÂMARA DOS DEPUTADOS. Promulgado decreto legislativo que aprova acordo internacional sobre crime cibernético. Disponível em: https://www.camara.leg.br/noticias/841844-promulgado-decreto-legislativo-que-aprova-acordo-internacional-sobre-crime-cibernetico/%20Epa!%20Vimos%20que%20voc%C3%AA%20copiou%20o%20texto.%20Sem%20problemas,%20desde%20que%20cite%20o%20link:%20https://www.migalhas.com.br/depeso/388700/efeitos-da-convencao-de-budapeste-nas-relacoes-juridicas-nacionais. Acesso em: 31 jun. 2023.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Rio de Janeiro: Jorge Zahar. 1. ed. 2003.

CASTELLS, Manuel. **A sociedade em rede** – A era da informação: economia, sociedade e cultura. Tradução: Roneide Venancio Majer. 24. ed. Rio de Janeiro: Paz e Terra, 2022.

CASTELLS, Manuel. **O espaço de fluxos: a nova geografia das resdes de poder. In: A sociedade em dere: A era da informação: economia, sociedade e cultura.** Volume II. São Paulo: Paz e Terra, 1999.

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, ago. 2021. ISSN 1984-7858. DOI: https://doi.org/10.26729/et.v21i1.3247.

COUNCIL OF EUROPE. Aderindo à Convenção de Budapeste sobre Cibercrime: Benefícios. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 31 jun. 2023.

FIGUEREDO, Alani Caroline Osowski; RIOS, Rodrigo Sánchez. Proteção de Dados e direitos fundamentais: desafios frente à cooperação jurídica internacional em matéria penal. Revista Científica doCPJM, Rio de Janeiro, Vol. 2, N.07, 2023. DOI: 10.55689/rcpjm.2023.07.006. ISSN: 2764-1899.

FONSECA, Marcos de Lucca; GENNARINI, Juliana Camarigo. A adesão do Brasil à Convenção de Budapeste e os impactos para a produção de provas digitais. **Revista de Direito Penal e Processo Penal**, v. 4, n. 1, jan./jun. 2022. ISSN 2674-6093.

FREITAS, Cinthia Obladen de Almendra; PIRATELLI, João Paulo Machado e SOUSA, Devilson da Rocha. A criptografia como mecanismo de proteção de provas digitais na cadeia de custódia. In: **CONGRESSO NACIONAL DO CONPEDI**, 25., 2016, Brasília. Anais […]. Florianópolis: CONPEDI, 2016. v. 5, p. 906-929.

GUARAGNI, Fábio André; RIOS, Rodrigo Sanchez. Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea. **Revista de estudos criminais**, Porto Alegre, v. 18, n. 73, p. 167-169, 2019.

KARPERSKY. O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos? Disponível em: https://www.kapersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 30 jul. 2023.

LOPES JÚNIOR, Aury. **Direito Processual Penal.** 17. ed. São Paulo: SaraivaJur, 2020.

MASSENA, Caio Badaró. A propósito da cadeia de custódia das provas digitais no processo penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa. Boletim do IBCCrim, ano 31, n. 368, julho/2023. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/issue/view/25/11>. Acesso em 30 jul. 2023.

MATILDA, Janaina. A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes. Boletim IBCCRIM. Ano 28, n. 331, jun. 2020, ISSN 1676-3661.

MURATA, Ana Maria Lumi Kamimura; TORRES, Paula Ritzmann. A Convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? Boletim IBCCRIM. Ano 31, n. 368, jul. 2023, ISSN 1676-3661.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. São Paulo: Marcial Pons, 2019.

SANTOS, Denise Tanaka dos Santos. **Delitos Informáticos: Convenção de Budapeste.**

SYDOW, Spenser Toth. **Curso de Direito Penal Informático:** partes geral e especial. 3. ed. Salvador: Editora JusPodivm, 2022.

USP, Jornal. Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano. Disponível em: <https://jornal.usp.br/radio-usp/brasil-sofreu-mais-de-100-bilhoes-de-tentativas-de-ataques-ciberneticos-no-ultimo-ano/>. Acesso em: 31 jun. 2023.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2020.