REVISTA DCS
FUNDADA EN 2000

DE BUDAPESTE À HANÓI: UMA ANÁLISE COMPARATIVA ENTRE OS TRATADOS INTERNACIONAIS DE COMBATE A CIBERCRIMES E SEUS DESAFIOS QUANTO AO ALCANCE UNIVERSAL E À PROTEÇÃO DE DIREITOS HUMANOS

FROM BUDAPEST TO HANOI: A COMPARATIVE ANALYSIS OF INTERNATIONAL TREATIES TO COMBAT CYBERCRIME AND THEIR CHALLENGES REGARDING UNIVERSAL REACH AND THE PROTECTION OF HUMAN RIGHTS

DE BUDAPEST A HANOI: UN ANÁLISIS COMPARATIVO DE LOS TRATADOS INTERNACIONALES DE LUCHA CONTRA EL CIBERCRIMEN Y SUS DESAFÍOS EN CUANTO A ALCANCE UNIVERSAL Y PROTECCIÓN DE LOS DERECHOS HUMANOS

Guilherme Simões Wanderley Lins[1]

DOI: 10.54899/dcs.v23i87.4667
Recibido: 19/01/2026 | Aceptado: 11/02/2026 | Publicación en línea: 19/02/2026.

RESUMO

Este artigo realiza uma análise comparativa entre a Convenção de Budapeste e a Convenção das Nações Unidas contra o Cibercrime (Convenção de Hanói), examinando as diferenças na tipificação penal, nos mecanismos de cooperação jurídica internacional e na proteção dos direitos humanos. O estudo adota uma abordagem qualitativa de natureza analítico-crítica, utilizando a técnica de análise documental de fontes primárias e o procedimento comparativo. Parte-se da hipótese de que a transição de um modelo regional para um tratado de vocação universal, embora necessária para a eficácia da cooperação global, impõe riscos de retrocessos nos direitos humanos devido às profundas tensões geopolíticas. Os resultados indicam que, enquanto a Convenção de Budapeste sofre com a falta de adesão de Rússia, China e Índia, o novo texto da ONU apresenta incertezas quanto à sua capacidade de universalização e fragilidades em relação à proteção de direitos humanos em decorrência de baixo quórum para adoção de protocolos adicionais.

Palavras-chave: Direito Internacional. Cibercrime. Convenção de Budapeste. Convenção de Hanói. Direitos Humanos.

ABSTRACT

This article conducts a comparative analysis between the Budapest Convention and the United Nations Convention against Cybercrime (the Hanoi Convention), examining the differences in criminalization, international legal cooperation mechanisms, and the protection of human rights. The study adopts a qualitative analytical-critical approach, utilizing document analysis of primary

[1] Pós-Graduado em Direito Internacional, Centro de Estudos em Direito e Negócios (CEDIN), Belo Horizonte, Minas Gerais, Brasil. E-mail: guilhermeswlins@gmail.com

sources and a comparative procedure. It is hypothesized that the transition from a regional model to a treaty with universal aspirations, while necessary for the effectiveness of global cooperation, poses risks of human rights setbacks due to deep geopolitical tensions. The results indicate that, while the Budapest Convention suffers from the lack of accession by Russia, China, and India, the new UN text presents uncertainties regarding its universalization capacity and fragilities in human rights protection resulting from the low quorum for the adoption of additional protocols.

Keywords: International Law. Cybercrime. Budapest Convention. Hanoi Convention. Human Rights.

RESUMEN

Este artículo presenta un análisis comparativo entre el Convenio de Budapest y la Convención de las Naciones Unidas contra la Ciberdelincuencia (Convención de Hanói), examinando las diferencias en la clasificación penal, los mecanismos de cooperación jurídica internacional y la protección de los derechos humanos. El estudio adopta un enfoque cualitativo, analítico-crítico, utilizando la técnica del análisis documental de fuentes primarias y el procedimiento comparativo. Se plantea la hipótesis de que la transición de un modelo regional a un tratado con vocación universal, si bien es necesaria para la eficacia de la cooperación global, conlleva riesgos de retrocesos en materia de derechos humanos debido a las profundas tensiones geopolíticas. Los resultados indican que, si bien el Convenio de Budapest adolece de la falta de adhesión de Rusia, China e India, el nuevo texto de la ONU presenta incertidumbres respecto a su capacidad de universalización y debilidades en relación con la protección de los derechos humanos debido al bajo quórum para la adopción de protocolos adicionales.

Palabras clave: Derecho Internacional. Ciberdelincuencia. Convenio de Budapest. Convenio de Hanói. Derechos Humanos.

INTRODUÇÃO

Conforme o 2022 Norton Cyber Safety Insights Report, mais de 415 milhões de pessoas em 10 países foram vítimas de cibercrimes[2] de janeiro de 2021 a janeiro de 2022. Tais delitos não costumam ficar limitados a fronteiras e exigem, por isso, que os Estados cooperem entre si, sobretudo com base em tratados internacionais, para que haja a efetiva investigação, persecução criminal e punição de eventuais envolvidos em práticas criminosas.

[2] A pesquisa define cibercrimes de uma forma ampla, abrangendo delitos como softwares maliciosos (vírus, *hacking*, *phishing scam*, *ramsomware* etc), acesso não autorizado de redes sociais ou *e-mail*, fraudes bancárias, furtos de identidade (*identity theft*), *creeping* e *stalking*. Os dez países citados são Austrália, Brasil, França, Alemanha, Índia, Itália, Japão, Nova Zelândia, Reino Unido e Estados Unidos (2022, p. 4).

Para refletir sobre esses tratados internacionais e a forma como abordam o enfrentamento de cibercrimes, este artigo começa com a apresentação dos critérios de caracterização de cibercrimes e de cooperação jurídica internacional, conforme a literatura atual sobre o tema. Na sequência, aborda, por meio de análise documental, os principais dispositivos a respeito desses dois temas e de direitos humanos contidos na Convenção de Budapeste e na Convenção da Organização das Nações Unidas (ONU) contra cibercrimes (Convenção de Hanói). Por fim, analisa os desafios que ambos os instrumentos internacionais enfrentam no combate aos cibercrimes em relação ao alcance universal e à proteção de direitos humanos.

REVISÃO DE LITERATURA

Cibercrimes

Os cibercrimes[3] são categorizados pela doutrina, em sua maioria, em duas ou três modalidades. A divisão tripartite, utilizada principalmente por países anglófonos (Estados Unidos, Canadá, Reino Unido e Austrália), decorre de classificação feita pelo Departamento de Justiça dos Estados Unidos entre crimes 1. em que o computador ou sistemas de computador são os alvos da ação, como *hacking*, *malware* ou *Denial-of-Service (DoS) attack*; 2. em que o computador é um meio para a prática delitiva, como *stalking*, violações de direitos autorais ou pornografia infantil; e 3. em que o computador é um aspecto incidental da conduta criminal por possibilitar a obtenção de provas, como *e-mails* enviados à vítima por um suspeito de homicídio (Clough, 2010, p. 10). Ainda que muito utilizada, essa divisão tripartite é criticável, pois permite que qualquer delito comum seja conceituado como cibercrime, bastando para tanto que se obtenham provas em um computador (Chawki, 2015, p. 5).

Por sua vez, a divisão bipartite é utilizada por organizações e doutrinadores em diferentes

[3] A terminologia para crimes relacionados à tecnologia da informação **não é tema sedimentado** nas convenções internacionais, nas doutrinas ou nas legislações internas dos países. Em língua portuguesa, essa dificuldade pode ser observada nos nomes conferidos às delegacias especializadas em tais delitos, chamados de "cibernéticos", "por meios eletrônicos", "tecnológicos" e "de alta tecnologia", conforme destaca Alessandro Gonçalves Barreto (2022, p. 48-49). Em língua inglesa, a problemática não é diferente, como explica Jonathan Clough (2010, p. 9), com o uso de termos como *virtual crime*, *digital crime* ou *high-tech crime*. Este artigo utiliza o termo "cibercrime" em conformidade não apenas com a doutrina jurídica, mas sobretudo com a Convenção de Budapeste, tratado internacional mais relevante em vigor sobre o assunto.

categorias[4,5]. A classificação adotada neste artigo foi criada pela *Serious and Organised Crime Strategy* (2013, p. 22) e apresentada pelo *Home Department* do Reino Unido a seu Parlamento:

> Os cibercrimes descrevem duas atividades criminais distintas, mas intensamente relacionadas: os **crimes ciberdependentes e os crimes possibilitados por meio cibernético.** Nessa estratégica, usamos cibercrime quando nos referimos aos dois tipos: caso contrário, fazemos a distinção entre eles.
> **- Crimes ciberdependentes (*Cyber-dependent crimes*)**: só podem ser cometidos por meio de computadores, redes de computadores ou outras formas de tecnologia da informação e da comunicação (TIC). Incluem a criação e a disseminação de *malware* para obter ganhos financeiros, para hackear dados pessoais ou industriais importantes e para ataques de *denial of service* a fim de causar danos à reputação.
> **- Crimes possibilitados por meio cibernético (*Cyber-enabled crimes*) (**como fraude, compra de drogas ilegais e exploração sexual de crianças) podem ser praticados dentro ou fora da internet, mas, na internet, podem ocorrer em uma escala e em uma velocidade sem precedentes (tradução nossa)[6].

Além de afastar a criticada hipótese de cibercrime contida na divisão tripartite (cibercrime por simples uso de prova digital), a classificação da *Serious and Organised Crime Strategy* foi amplamente utilizado durante as negociações que deram origem à Convenção das Nações Unidas contra cibercrimes, assinada em 2025 em Hanói, no Vietnã. Um dos assuntos em debate foi o rol de crimes a serem positivados por essa norma internacional, motivo pelo qual é imprescindível analisá-la neste artigo.

COOPERAÇÃO JURÍDICA INTERNACIONAL

Em uma definição abrangente, a cooperação jurídica internacional[7] é o conjunto de atos

[4] Por exemplo, o Décimo Congresso da ONU de Prevenção ao Crime e Tratamento de Delinquentes (atualmente Prevenção ao Crime e Justiça Criminal) criou as categorias *in a narrow sense*, em que sistemas de computador e os dados por ele processados são alvos de ação ilegal; e *in a broader sense*, em que são crimes quaisquer condutas que possuam como meio sistemas de computador ou rede ou com eles se relacionem (Chawki, 2015, p. 6).

[5] No mesmo sentido, parte da doutrina brasileira adota a classificação bipartite com diferentes critérios, como crimes informáticos comuns e específicos e cibercrimes próprios e impróprios, similarmente à classificação de crimes militares (Albuquerque, 2006, p. 40). Crimes próprios são aqueles que afetam bens jurídicos relacionados à tecnologia da informação; e impróprios, crimes comuns que utilizam a tecnologia da informação como meio para a prática delitiva (Barreto, 2022, p. 54).

[6] No original: "*Cybercrime describes two distinct, but closely related, criminal activities: cyber-dependent crimes, and cyber-enabled crimes. In this strategy, we use 'cybercrime' when we are referring to both types: otherwise we distinguish between them.* • ***Cyber-dependent crimes*** *can only be committed using computers, computer networks or other forms of information communication technology (ICT). They include the creation and spread of malware for financial gain, hacking to steal important personal or industry data and denial of service attacks to cause reputational damage.* • ***Cyber-enabled crimes*** *(such as fraud, the purchasing of illegal drugs and child sexual exploitation) can be conducted on or offline, but online may take place at unprecedented scale and speed".*

[7] Também não há consenso sobre como designar a cooperação entre Estados em questões jurídicas. O presente artigo opta por "cooperação jurídica internacional" por ser o termo dominante na literatura jurídica e mais abrangente que as expressões que utilizam "judiciário" ou "jurisdicional", pois abarca cooperações administrativas (Bechara, 2009,

que normatizam a relação entre Estados ou entre Estados e tribunais internacionais, em razão dos limites territoriais da soberania (Bechara, 2009, p. 30).

A cooperação jurídica internacional pode ser sistematizada com base em diferentes critérios, por exemplo, os propostos por Fábio Ramazzini Bechara (2009, p. 33-34): 1. a iniciativa na solicitação (ativa, por ser solicitada por alguém, ou passiva, a quem se solicita); 2. a qualidade do cooperador (autoridades judiciais ou não judiciais); 3. a finalidade da cooperação (assistência simples, como notificações e produção de provas; medidas com possíveis resultados patrimoniais graves, como sequestro de bens; e medidas com possíveis resultados graves aos direitos fundamentais, como a extradição); e 4. o procedimento adotado (extradição, homologação de sentença estrangeira, carta rogatória ou auxílio direto).

Como se pode observar, essa cooperação pode envolver diferentes ramos do direito. Entre eles, encontra-se a matéria penal, que pode utilizar a cooperação jurídica internacional tanto durante a fase investigativa como no curso de processos penais.

Para que a cooperação entre os países possa ocorrer, deve haver uma promessa de reciprocidade entre Estados ou um acordo formal ou costume internacional. Os acordos formais podem ser feitos por meio de tratados bilaterais ou multilaterais[8] (Bechara, 2009, p. 35-36) e exigem uma concordância mínima entre os Estados que buscam a cooperação. É importante mencionar que países cooperantes podem advir de tradições jurídicas distintas (*civil law* ou *common law)*, com sistemas jurídicos em que as tipificações penais e regras processuais possuem mais diferenças que semelhanças, sendo benéfico que haja regras claras e precisas contidas em um instrumento internacional para que a cooperação ocorra de forma padronizada, válida e sem excessivas burocracias.

Os acordos internacionais destacam-se entre os meios de cooperação internacional, pois podem promover a harmonização de legislações internas e a proteção dos direitos humanos, com a fixação de garantias processuais mínimas[9] (Bechara, 2009, p. 45-46). Além disso, os tratados

p. 31).

[8] Exemplos de instrumentos multilaterais em matéria criminal são a Decisão-Quadro 2008/978/JAI, do Conselho Europeu, que regulamenta o mandato de utilização de provas naquele continente (Müller, 2013, p. 124); o Protocolo de Assistência Jurídica Mútua em Assuntos Penais do Mercosul e a Convenção Interamericana sobre Assistência em Matéria Penal, nas Américas; e, entre países de língua portuguesa, a Convenção de Auxílio Judiciário em Matéria Penal entre os Estados Membros da CPLP (Barreto, 2022, p. 116). No âmbito da ONU, foram criados instrumentos jurídicos a respeito de delitos transnacionais que trazem regras específicas de cooperação jurídica internacional, como a Convenção das Nações Unidas contra o Crime Organizado Transnacional e a Convenção das Nações Unidas contra a Corrupção (Barreto, 2022, p. 116-118).

[9] Segundo Bechara, há um rol de garantias processuais mínimas que devem ser positivadas pelos Estados: "[…] direito à prova; presunção de inocência; contraditório; defesa; duração razoável do processo; assistência gratuita do intérprete; respeito à intimidade, vida privada e familiar e inviolabilidade do domicílio" (2009, p. 80-81).

podem dar celeridade aos atos de cooperação internacional ao flexibilizar restrições estatais, como regras de dupla criminalização[10], e permitir o instituto do auxílio direto, realizado diretamente entre órgãos centrais de cada país, por vezes sem a necessidade de decisão judicial (Müller, 2013, p. 65-66).

Em relação aos cibercrimes, os desafios de cooperação e combate a infrações penais são ainda maiores. Tais delitos possuem uma lógica que ultrapassa fronteiras, em que um crime pode ocorrer com a presença do agente em um país e da vítima em outro, podendo as provas digitais estar armazenadas em um terceiro Estado[11]. Desse modo, fez-se necessária a regulamentação específica de cibercrimes em tratados internacionais, tema abordado pela Convenção de Budapeste, originado de propostas de países europeus, e recentemente pela Convenção de Hanói, no âmbito da ONU. A convenção e o projeto serão analisados a seguir.

METODOLOGIA

A presente pesquisa adota uma abordagem qualitativa de natureza teórica e documental, fundamentada no método analítico-crítico para examinar as tensões normativas e políticas na regulação internacional do cibercrime. Em relação a esse método, trago à baila as contribuições de Andréa Depiere de A. Reginato, em menção a McCullogh (Machado, 2017):

> Citando Jupp and Norris, McCullogh (2004, p. 39) recupera três perspectivas teóricas (consideradas de forma ampla) a partir das quais normalmente se situa a análise documental: positivista, interpretativa e crítica.
>
> A perspectiva positivista enfatiza a natureza objetiva, racional, sistemática e quantitativa do estudo. A perspectiva interpretativa destaca a natureza dos fenômenos sociais e os documentos como sendo socialmente construídos. **A tradição crítica é fortemente teórica e de natureza abertamente política, enfatizando conflito social, poder, controle e ideologia, inclui as teorias Marxista e Feminista e, mais recentemente, os modos críticos de análise do discurso**. (McCullogh, 2004, p. 39, tradução da autora) (grifo nosso)

[10] Bechara assim define a dupla incriminação: "[…] exigência de que o fato objeto da cooperação seja qualificado como infração penal na legislação dos Estados cooperantes, bastando a convergência dos elementos essenciais e pouco importando o *nomen iuris* e a presença de outros elementos" (2009, p. 139).

[11] Como explica Jonathan Clough (2012, p. 365): "the interconnected nature of the technology means that this is a global problem. Modern computer networks have challenged the traditional view that criminal law is local in nature. As individuals may now communicate overseas as easily as next door, offenders may be present, and cause harm, anywhere there is an Internet connection. Even where offender and victim are in the same jurisdiction, the nature of networked communications means that data will routinely be routed through, or stored in, multiple jurisdictions. Not only does this provide, literally, a world of opportunity for offenders, it presents enormous challenges to law enforcement".

Quanto aos objetivos, o estudo caracteriza-se como exploratório qualitativo (Machado, 2017), buscando detalhar as peculiaridades e desafios contidos na Convenção de Budapeste e na Convenção da ONU.

A técnica central de investigação consiste na análise documental, abrangendo fontes primárias, como os textos integrais dos tratados, além de fontes secundárias baseadas em literatura especializada e relatórios técnicos de órgãos internacionais. Quanto a isso, segue a explicação de Andréa Depiere de A. Reginato (Machado, 2017):

> 1. Fontes primárias – são todas aquelas que permitem ao pesquisador se aproximar ao máximo do evento pesquisado, de ideias originais ou ainda dos resultados de uma pesquisa empírica. Essas fontes podem incluir documentos originais, trabalhos criativos, relatos produzidos em primeira mão ou mesmo a publicação dos resultados diretos de uma pesquisa empírica. As fontes primárias resultam da participação ou observação direta dos fatos.
> 2. Fontes secundárias – são aquelas que se dedicam à análise, revisão, sistematização ou resumo das informações decorrentes de uma fonte primária ou mesmo de fontes secundárias. É muito comum que fontes secundárias interajam entre si e que mobilizem os esforços teóricos típicos de uma área do saber para alcançar resultados. As fontes secundárias se constituem como as principais fontes de análise e interpretação das fontes primárias.

O procedimento lógico de análise é o método comparativo, estruturado em torno de categorias como tipificação penal, mecanismos de cooperação jurídica e salvaguardas de direitos humanos, com o intuito de identificar convergências, divergências geopolíticas e possíveis riscos à proteção de garantias fundamentais no cenário digital global.

ANÁLISE E DISCUSSÃO

A Convenção de Budapeste

A Convenção de Budapeste, formulada em 2001 e em vigor desde 1º de julho de 2004, foi instituída no seio do Conselho da Europa e é o primeiro tratado internacional a tratar de cibercrimes (Council of Europe, 2001). Tem como origem os estudos realizados sobre o tema por um grupo de especialistas constituído em 1996 pelo Comitê Europeu para os Problemas Criminais (CDPC), que elaborou o projeto inicial da Convenção. O acordo foi aprovado em seguida ao atentado terrorista de 11 de setembro de 2001, no contexto de prevenção e combate de crimes transnacionais, os quais exigiram ampla cooperação global (Brito, 2013, p. 47).

Os três objetivos da Convenção de Budapeste foram assim condensados por Auriney Brito

(2013, p. 56):

> […] (a) harmonizar a tipicidade penal no ambiente do ciberespaço pelos Estados signatários; (b) definir os elementos do sistema de informática promovendo a unidade na interpretação da legislação penal interna e possibilitar a credibilidade da prova eletrônica no ambiente virtual; (c) implementar um sistema rápido e eficaz de cooperação internacional no combate à criminalidade de informática.

Esse tratado possui 48 artigos e divide-se em quatro capítulos: I – Terminologia[12]; II – medidas a serem adotadas pelos países signatários; III – cooperação internacional; e IV – disposições finais[13]. O presente estudo foca as medidas a serem adotadas pelos países, sobretudo os tipos penais, a cooperação internacional e a proteção de direitos humanos.

Quanto às medidas adotadas por legislações dos Estados Partes, o tratado determina aos signatários a inclusão de tipos penais, na seção 1; de medidas e procedimentos, na seção 2; e de regras de jurisdição, na seção 3. A fim de manter o enfoque do presente artigo, iniciemos por breve resumo das seções 2 e 3, nas palavras de Alessandro Gonçalves Barreto (2022, p. 102):

> […] versa sobre condições e salvaguardas, conservação expedita de dados informáticos e sua busca e apreensão, injunção, recolhimento, em tempo real, de dados informáticos e interceptação de dados relativos ao conteúdo, afora competência e cooperação internacional.

Na seção 1, os tipos penais são divididos em quatro títulos e somente podem ser cometidos na forma dolosa. O primeiro título[14] refere-se a crimes ciberdependentes, enquanto os demais se referem a crimes possibilitados por meio cibernético, com crimes informáticos no segundo título[15]; crimes relacionados à pornografia infantil no terceiro título[16]; e crimes referentes a

[12] O tratado uniformiza quatro nomes básicos de tecnologia da informação e a interpretação dada a eles pelos países signatários em suas legislações nacionais (Brito, 2013, p. 56). Assim, em seu artigo 1º, define o que são "sistema de computador", "dado de computador", provedor de serviço" e "dados de tráfego".

[13] É importante ressaltar o artigo 37, que determina a possibilidade de adesão à Convenção de membros não participantes do Conselho da Europa, desde que ocorra após decisão de convidá-los, por voto unânime, em quórum majoritário dos Estados convenentes com assento no Conselho de Ministros.

[14] O primeiro título trata de "crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador", contidos nos artigos 2 a 6 do tratado. São eles: acesso ilegal a sistema; interceptação ilícita de dados; violação (danificação, eliminação, deterioração, alteração ou supressão dolosa) de dados; interferência (grave obstrução ou impedimento não autorizados) em sistema; e uso indevido de aparelhagem. Esses delitos são caracterizados pelo fato de que a própria tecnologia é o alvo da ação (Clough, 2012, p. 372).

[15] O segundo título, denominado de "crimes informáticos", é formado pelos artigos 7 e 8: falsificação informática (inserção, alteração, apagamento ou supressão de dados para aparentar legalidade); e fraude informática (inserção, alteração, apagamento ou supressão de dados ou interferência no funcionamento do computador que cause prejuízo patrimonial).

[16] O terceiro título refere-se ao crime relacionado ao conteúdo. Nessa toada, a Convenção restringe-se ao combate da pornografia infantil, buscando punir condutas como a produção, o oferecimento, a disponibilidade, a aquisição ou

direitos autorais e correlatos no quarto título[17,18].

Em relação aos mecanismos de cooperação internacional[19] contidos nessa Convenção, Clough (2012, p. 371) explica:

> O Capítulo III da Convenção dedica-se à cooperação internacional, particularmente nas áreas de extradição e auxílio mútuo. Estabelece o princípio geral de que as partes cooperarão entre si "na maior medida possível" na investigação de cibercrimes e na coleta de evidências eletrônicas (artigo 23). Isso inclui o compartilhamento espontâneo de informações, sem solicitação prévia, quando estas puderem auxiliar outra parte em sua investigação (artigo 26). As partes devem, ainda, estabelecer um ponto de contato operante 24 horas por dia, 7 dias por semana, com a finalidade de prestar assistência em investigações de crimes cibernéticos (artigo 35).
> Há também previsões para o auxílio mútuo que espelham os poderes processuais discutidos anteriormente. Notadamente, considerando que as evidências podem ser eliminadas durante o trâmite pelos canais tradicionais, o texto prevê a preservação célere de dados informáticos armazenados e a revelação célere de dados de tráfego (artigos 29 e 30). Tais medidas permitem assegurar a prova ou verificar o fluxo das comunicações enquanto se aguardam solicitações complementares. No tocante à coleta de dados de tráfego em tempo real e à interceptação de dados de conteúdo, as partes prestarão a assistência permitida por suas legislações internas e tratados aplicáveis (artigos 33 e 34)[20].

Além das citadas previsões de extradição e auxílio direto, com mitigações à dupla incriminação[21], Gregor Urbas ressalta que a Convenção possibilita que países sem relações

a posse de materiais relacionados à pornografia infantil.

[17] O quarto título aborda "violações de direitos autorais e de direitos correlatos", relacionando os delitos às obrigações impostas em outros tratados internacionais, como o Ato de Paris, de 24 de julho de 1971, e a Convenção Internacional para a Proteção de Artistas, Produtores de Fonogramas e Organizações Radiodifusoras, assinada em Roma (Convenção de Roma). Conforme esclarece Gregor Urbas, "[…] The Convention on Cybercrime deals only with infringements of copyright and related rights, the latter relating to broadcasting services rather than moral rights" (2019, p. 320).

[18] Outros crimes estão previstos em Protocolo Adicional à Convenção, que trata do combate ao racismo e à xenofobia. Disponível em: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm. Acesso em: 21 fev. 2023.

[19] O 2º Protocolo Adicional à Convenção, ainda em fase de assinatura e ratificação pelos países, prevê meios de aprimorar a cooperação jurídica internacional e divulgar provas eletrônicas. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224. Acesso em: 21 fev. 2023.

[20] No original (2012, p. 371): "*Chapter III of the Convention is concerned with international cooperation, particularly in the areas of extradition and mutual assistance. It states the general principle that parties will cooperate with each other "to the widest extent possible" in the investigation of cybercrimes and the collection of electronic evidence (article 23). This includes the sharing of information without request where it would assist another party in its investigation (article 26). Parties are also to establish a 24/7 contact point for the purpose of providing assistance in relation to cybercrime investigations (article 35). Provision is also made for mutual assistance, mirroring the procedural powers discussed above. In particular, given that evidence may be deleted by the time traditional channels are pursued, provision is made for expedited preservation of stored computer data and expedited disclosure of traffic data (articles 29 and 30). This allows evidence to be secured, or the path of communications ascertained, pending further requests. In the case of real time collection of traffic data and interception of content data, parties shall give such assistance as permitted under their domestic laws and applicable treaties (articles 33 and 34).*

[21] Por exemplo, cite-se o artigo 29, "3", da Convenção: "3. Ao receber o pedido de outra Parte, a Parte requerida adotará todas as medidas apropriadas para conservar, com presteza, os dados especificados, de acordo com sua legislação doméstica. **Para resposta a um pedido de assistência, o princípio da dupla tipicidade não será exigido**

bilaterais a utilizem como base de cooperação internacional (2019, p. 325), tudo com o fim de evitar a impunidade relacionada à prática de cibercrimes.

Por fim, o acordo declara a necessidade de respeitar os direitos humanos fundamentais em seu artigo 15, no dispositivo transcrito abaixo:

> 1. Cada Parte assegurará que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos nesta seção sujeitem-se às condições e garantias instituídas na sua legislação interna, **que estabelecerá proteção adequada aos direitos humanos e às liberdades públicas, incluindo os direitos nascidos em conformidade com as obrigações que esse Estado tenha assumido** na Convenção do Conselho da Europa para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, de 1950, na Convenção Internacional da ONU sobre Direitos Civis e Políticos, de 1966, **e em outros instrumentos internacionais de direitos humanos, e que tais poderes e procedimentos incorporarão o princípio da proporcionalidade** (grifos nossos).

Feito esse breve delineamento da Convenção de Budapeste, passa-se agora à análise da Convenção de Hanói para, em seguida, analisar os desafios que ambos os instrumentos internacionais enfrentam.

A CONVENÇÃO DE HANÓI

As negociações no âmbito da ONU dividem-se, desde sua origem, em dois temas de segurança cibernética[22]: ciberguerras e cibercrimes. De forma resumida, a negociação sobre ciberguerras aborda questões político-militares entre Estados e ocorre, sobretudo, no âmbito da Primeira Comissão da Assembleia Geral das Nações Unidas (AGNU). Já o debate sobre enfretamento de cibercrimes ocorre, especialmente, no âmbito da Terceira Comissão da AGNU (Maurer, 2011, p. 15).

Em relação aos cibercrimes, a iniciativa das negociações partiu da Rússia, que propôs, em 16 de novembro de 2000, a Resolução A/55/59, intitulada "Combatendo o Uso Indevido das Tecnologias da Informação para Fins Criminosos"[23] (Maurer, 2011, p. 35). Em 27 de dezembro de 2019, a AGNU aprovou, também por iniciativa russa, a formação de um comitê *ad hoc*, com

como condição para autorizar a conservação de dados" (grifo nosso).

[22] Como explica Tim Maurer (2011, p. 16), há quem entenda que existe uma terceira discussão sobre cibersegurança a respeito de governança da internet. O autor, no entanto, considera que essa discussão apenas tangencia a cibersegurança, tratando-a de forma limitada, motivo pelo qual não a leva em conta em sua divisão bipartite. As negociações sobre governança da internet ficam a cargo do Fórum de Governança da Internet e da 2ª Comissão da AGNU.

[23] No original (Maurer, 2011): *Combating the Criminal Misuse of Information Technologies.*

o apoio do Escritório das Nações Unidas sobre Drogas e Crimes (UNODC), para elaborar uma ampla convenção internacional sobre o enfrentamento do uso de tecnologia de informação e comunicação para fins criminais, a A/RES/74/247 (United Nations, 2019b). Esse comitê ficou responsável por negociar a elaboração de um tratado sobre cibercrimes em seis sessões, com previsão de conclusão em fevereiro de 2024 (United Nations, 2022).

A base do projeto da Convenção da ONU contra Cibercrimes foi delineada em sessões do comitê *ad hoc*, ocorridas a partir de 2022, com fundamento em sugestões dos Estados-membros (Bannelier, 2023). Já o texto final, adotado pela Assembleia Geral da ONU em 24 de dezembro de 2024 pela Resolução 79/243, foi assinado por 74 (setenta e quatro) países em 25 de outubro 2025, na cidade de Hanói, no Vietnã (United Nations, 2025). O projeto, durante esse período, passou por inúmeras idas e voltas, alcançando-se um improvável consenso. Do que foi concluído, alguns pontos merecem destaque, como o nome da Convenção, os crimes, a proteção aos direitos humanos e a cooperação internacional.

Em termos gerais, os debates estavam polarizados entre um grupo que apoiou as ideias da Rússia e da China e outro que aderiu às ideias dos Estados Unidos e de países da União Europeia (Bannelier, 2023). Com base nas declarações dos países veiculadas nos documentos da Assembleia Geral (A/74/130) e do comitê ad hoc (A/AC.291/4), Rússia e China defenderam um tratado amplo que tratasse de prevenção e punição de crimes relacionados ao uso da tecnologia da informação, com dispositivos expressos de proteção à soberania dos países[24]. Por outro lado, países da União Europeia e Estados Unidos pretendiam um tratado que definisse cibercrimes da forma mais restrita possível, limitando-se à repressão de crimes[25], à cooperação jurídica, à proteção de direitos humanos e a disposições convergentes com a Convenção de Budapeste (United Nations, 2021)[26].

A polarização se iniciou com o nome da Convenção. O primeiro grupo propôs um nome

[24] Conforme notas da Assembleia Geral (A/74/130), a Rússia alegou que a Convenção de Budapeste permite violações à soberania e interfere em assuntos internos dos países. Por isso, argumenta que há a ameaça de o projeto da ONU legitimar o acesso de dados pessoais de usuários de todo o mundo por serviços especiais de um limitado grupo de países. O país reitera ainda o risco de o projeto consolidar os ganhos tecnológicos de países desenvolvidos, mantendo a "lacuna digital" entre esses países e países em desenvolvimento (United Nations, 2019a, p. 59).

[25] Conforme notas do comitê *ad hoc* (A/AC.291/4), os Estados Unidos entendiam que a convenção deve ser limitada a um instrumento de justiça criminal e não abordar outros temas relacionados à cibersegurança, como normas de comportamento não criminais na internet e outras normas de governança (United Nations, 2021, p. 64).

[26] Cumpre salientar que um terceiro posicionamento surgiu durante os debates, denominado de "países do meio", formada principalmente por Estados do Caribe e da África, que buscavam uma convenção que oferecesse acesso à cooperação, à capacitação e à assistência técnica em matéria de cibercrimes. Além disso, os debates do projeto tiveram ampla participação da sociedade civil, seja de empresas do setor de tecnologia, seja de defensores de direitos humanos, o que muito contribuiu para a finalização do tratado (Bannelier; Lostri, 2024).

mais genérico, "Convenção Internacional Abrangente sobre o Combate à Utilização de Tecnologias de Informação e Comunicação para Fins Criminosos" e o segundo defendeu o título "Convenção da ONU contra Cibercrimes" [27] (Bannelier, 2023). Venceu a longa denominação "Convenção das Nações Unidas contra o Cibercrime; Fortalecimento da Cooperação Internacional para o Combate a Certos Crimes Cometidos por Meio de Sistemas de Tecnologias de Informação e Comunicação e para o Compartilhamento de Provas em Formato Eletrônico de Crimes Graves[28]" (United Nations, 2025), em mesclagem que buscou conciliar interesses de todos os grupos participantes. De toda maneira, o tratado tem sido comumente chamado de "Convenção da ONU contra os Cibercrimes" ou "Convenção de Hanói".

Em relação à definição de crimes, Rússia e China propuseram um amplo rol de delitos relacionados à tecnologia da informação, inclusive crimes possibilitados por meio cibernético, como a distribuição de substâncias psicotrópicas e o tráfico de armas. Por sua vez, o grupo formado pelos Estados Unidos e países da Europa pretendia que o tratado deveria abranger os crimes ciberdependentes e algumas exceções de crimes possibilitados por meio cibernético (United Nations, 2021) [29].

A Convenção foi concluída com um escopo limitado de tipos penais, muito próximos ao que previstos na Convenção de Budapeste e ao que pretendido pelo grupo apoiado por Estados Unidos e União Europeia. Tais delitos estão estabelecido no Capítulo 2 – Criminalização, entre os artigos 7 a 21, e determinam aos Estados que tipifiquem hipóteses de crimes ciberdependentes, como acesso ilegal (artigo 7) e interceptação ilegal (artigo 8) de qualquer sistema tecnológico de informação e comunicação; e crimes possibilitados por meio cibernético, como o sancionamento de condutas relacionadas ao abuso sexual infantil online ou a material de exploração sexual infantil (artigo 14) e à disseminação não consensual de imagens íntimas (artigo 16) (United Nations, 2025)[30].

Em relação à cooperação jurídica, a Convenção estabeleceu, em seu Capítulo V, artigos

[27] No original: "*Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes"* e "*U.N. Convention against Cybercrime*" (United Nations, 2022).

[28] No original: "*United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*" (United Nations, 2025).

[29] Conforme notas do comitê *ad hoc* (A/AC.291/4), os Estados Unidos defenderam a criminalização de condutas relacionadas à pornografia infantil, a fraudes bancárias e a direitos autorais (United Nations, 2021, p. 66).

[30] Segundo Karine Bannelier e Eugenia Lostri, a limitação dos artigos foi uma vitória específica do Reino Unido, do Japão e da França, que foram contrários à inclusão de dispositivos que criminalizassem a desinformação, pois entendiam que tais previsões poderiam ser utilizadas por países autoritários para fins indevidos, como punir dissidentes (2024).

35 a 52, uma sistemática bastante abrangente, incluindo disposições a respeito de extradição, da rede 24/7, de recuperação de bens, de investigações conjuntas, de coleta e de preservação de dados.

Necessário frisar que a previsão de cooperação internacional em termos de aplicação da lei (e, com isso, a punição de crimes), no artigo 35, abarca não apenas cibercrimes, mas também "crimes graves", que são aqueles que puníveis com pena mínima de 4 (quatro) anos, conforme art. 2º, alínea "h".

Por fim, um ponto divergente nas discussões do tratado era a respeito da proteção de direitos humanos, por ausência de uma previsão no texto inicial proposto pela Rússia e na dificuldade de inclusão expressa do tema pela segunda coalisão. Após os debates, chegou-se a um dispositivo genérico:

> Artigo 6: Respeito aos direitos humanos
> 1. Os Estados-Partes assegurarão que o cumprimento de suas obrigações nos termos desta Convenção seja compatível com suas obrigações decorrentes do direito internacional dos direitos humanos.
> 2. Nada nesta Convenção deverá ser interpretado de forma a permitir a supressão de direitos humanos ou liberdades fundamentais, inclusive os direitos relacionados às liberdades de expressão, consciência, opinião, religião ou crença, reunião pacífica e associação, em conformidade e de maneira compatível com o direito internacional dos direitos humanos aplicável (tradução nossa.)31

Tal disposição foi objeto de diferentes críticas. Entre elas, a Autoridade Europeia para a Proteção de Dados (com a sigla em inglês EDPS) apresentou a opinião 23/25 em que aponta a ausência de previsão expressa quanto ao direito à privacidade e à proteção de dados de usuários (2025, p. 3):

> A Autoridade Europeia para a Proteção de Dados (EDPS) recorda o vasto número de países integrantes das Nações Unidas e os seus sistemas jurídicos altamente heterogêneos no que tange ao respeito aos direitos e liberdades fundamentais, incluindo os direitos fundamentais à privacidade e à proteção de dados. Diante desse cenário, o EDPS considera de suma importância assegurar que a cooperação com países terceiros sob a égide da Convenção não resulte no enfraquecimento ou prejuízo à proteção dos direitos e liberdades fundamentais das pessoas naturais garantidos pela legislação da União Europeia, em particular os seus direitos à proteção de dados e à privacidade

[31] No original: "Article 6: Respect for human rights
1. States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law.
2. Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law".

(tradução nossa)[32].

Ademais, o artigo 24 previu, em relação à proteção de direitos humanos, o princípio da proporcionalidade, em conformidade com o Direito Internacional aplicável em matéria de Direitos Humanos[33].

Note-se, portanto, que a Convenção de Hanói é um instrumento jurídico que encampou interesses muito divergentes e que, a despeito de uma concordância em seu texto final, possui alguns obstáculos a serem enfrentados no futuro com sua implementação. Feito esse breve panorama, o próximo tópico tratará dos desafios a serem enfrentados tanto pela Convenção de Budapeste como pela Convenção de Hanói como instrumentos universais de combate aos cibercrimes e em relação à proteção de direitos humanos.

DESAFIOS ENFRENTADOS PELA CONVENÇÃO DE BUDAPESTE E PELA CONVENÇÃO DE HANÓI

Em relação à Convenção de Budapeste, existem desafios a respeito de sua capacidade de universalização e sua desatualização frente a novas tecnologias.

Criada em 2001, a Convenção de Budapeste possui atualmente 81 Estados partes (Council of Europe, 2001)[34]. Entre os países que a adotaram estão Estados Unidos, Alemanha, França, Reino Unido, Japão, Austrália, Argentina, Paraguai, Chile e Brasil. Além disso, o acordo conta com 15 países observadores, como África do Sul e México; e 11 organizações observadoras do Comitê da Convenção de Cibercrimes, como a Comissão da União Africana, a Organização dos Estados Americanos e o UNODC. A despeito da larga abrangência do acordo, não são Estados partes países asiáticos como a Rússia, a China e a Índia, que se negam a aderir ao tratado por não terem participado de suas negociações (Pavlova, 2025).

[32] No original: “The EDPS recalls the vast number of countries within the United Nations and their highly heterogeneous legal systems as regard the respect of fundamental rights and freedoms, including the fundamental rights to privacy and data protection. Against this background, the EDPS considers of paramount importance to ensure that cooperation with third countries under the Convention does not lead to weakening or otherwise prejudicing the protection of fundamental rights and freedoms of natural persons guaranteed under EU law, in particular their rights to data protection and privacy”.

[33] Entre as críticas ao artigo, a Fundação para Defesa de Democracias (FDD) reiterou que o termo “aplicável” permite que os países decidam por conta própria quais tratados internacionais seriam aplicáveis. Em contraposição, a Convenção de Budapeste refere-se especificamente aos direitos contidos no Pacto Internacional dos Direitos Civis e Políticos de 1966 (Stradner; Hester, 2025).

[34] Rol de Estados-Partes que ratificaram a Convenção disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. Acesso em: 04 fev. 2026.

Mohamed Chawki reforça a necessidade de adesão de países árabes à convenção e de auxílio a países para que criem estruturas administrativas de enfretamento de cibercrimes, sob pena de formação de refúgios para crimes (*crime shelters)* (2015, p. 22-23). Do mesmo modo, Lennon Yao-Chung Chang ressalta que é preciso diminuir a barreira entre países desenvolvidos e em desenvolvimento. Para tanto, exemplifica que Estados como Mianmar, Laos e Camboja carecem de auxílio para construir um arcabouço de cibersegurança para lidar com cibercrimes, ainda diminuto na Península Indochinesa (2019, p. 341).

A respeito de desafios sobre a desatualização frente a novas tecnologias, Clough faz os seguintes apontamentos (2012, p. 378-379):

> Dado o ritmo das mudanças desde que a Convenção foi redigida, é de se esperar que tenham surgido novas formas de criminalidade que não foram incluídas. A discussão a seguir foca em quatro categorias de delitos: **furto de identidade, *grooming* (aliciamento), spam e ciberterrorismo**. Antes de considerar esses delitos, é importante distinguir entre as infrações que não foram antecipadas no momento da redação e aquelas sobre as quais não foi possível alcançar um consenso internacional. Enquanto as primeiras podem ser incorporadas em uma convenção emendada ou nova, as últimas limitarão necessariamente o escopo de qualquer convenção sobre cibercrime (tradução e grifo nosso)[35].

Embora demonstre ausência de tipificação penal de novos delitos, como aliciamento de crianças pela internet e ciberterrorismo, o autor esclarece que a própria Convenção possui meios de se atualizar e normatizá-los, tanto por meio de emendas como de protocolos adicionais (Clough, 2012, p. 379).

A Convenção da ONU também enfrenta desafios quanto à capacidade de universalização. Além disso, há obstáculos em relação à conformação de interesses diversos entre seus signatários e ao incremento de normas que possam comprometer a proteção de direitos humanos e a cooperação jurídica internacional.

Apesar de já ter sido assinada por 74 (setenta e quatro) países[36]e, entre eles, China e Rússia, é cedo para se afirmar que a Convenção será adotada de forma ampla por países da ONU.

[35] No original: "Given the pace of change since the Convention was drafted, it is to be expected that new forms of offending would have arisen which were not included. The following discussion focuses on four categories of offence; identity theft, grooming, spam and cyberterrorism. Before considering these offences it is important to distinguish between those offences which were not anticipated at the time of drafting, and those on which international agreement could not be reached. While the former may be incorporated within an amended or new convention, the latter will necessarily limit the scope of any cybercrime convention".

[36] Rol de Estados-Partes que ratificaram a Convenção disponível em: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en. Acesso em: 04 fev. 2026.

A recente Convenção pende de ratificação dos países signatários e entrará em vigor 90 (noventa) dias após o 40º (quadragésimo) depósito de instrumento de adoção de Estados signatários, conforme seu artigo 60 (1). Nesse sentido, não se sabe, por ora, quantos países irão adotar em definitivo o referido instrumento.

Outro importante desafio desta Convenção se refere à possibilidade de criar protocolos adicionais por meio da aprovação de dois terços dos Estados-Partes, em seus artigos 61 e 62. Tal flexibilização poderia permitir a adoção de protocolos para atendimento de interesses de apenas um dos blocos de países. Nas palavras de Karine Bannelier e Eugenia Lostri (2024):

> Embora a batalha possa ter sido ganha, a guerra continua. Aqueles crimes preocupantes ainda podem encontrar espaço no escopo da convenção. Os Artigos 61 e 62 preveem que a Conferência dos Estados Partes poderá suplementar a convenção com um ou mais protocolos adicionais. Esses protocolos precisam apenas ser submetidos por pelo menos 60 Estados e, embora devam preferencialmente ser adotados por consenso, uma votação de maioria de dois terços dos estados partes presentes e votantes seria suficiente para a sua adoção. Isso significa que nada impede que a Rússia ou a China, com o apoio de 60 estados, proponham a adoção de um protocolo que inclua uma disposição contra crimes relacionados ao extremismo — abrindo as portas para amplas interpretações domésticas. A negociadora-chefe dos EUA, a Embaixadora Deborah McCarthy, argumentou que foi uma vitória duramente conquistada para a equipe dos EUA e seus aliados e parceiros conseguir estabelecer um patamar elevado para a negociação de um protocolo, contra a oposição constante de estados com inclinações mais autoritárias. É verdade que a Rússia e a China originalmente queriam que um número menor de países fosse suficiente para viabilizar e adotar um protocolo. Foi, de fato, uma solução de compromisso elevar o número para 60 estados. No entanto, permanece a possibilidade de que um grupo não tão numeroso de países expanda desarrazoadamente o escopo da convenção e ameace liberdades fundamentais. Os Artigos 61 e 62 pairam sobre as liberdades fundamentais e exigirão vigilância inabalável e contínua por parte dos estados democráticos e da sociedade civil (tradução nossa)[37].

É notório que alguns países se utilizam de suas legislações domésticas para supressão de direitos humanos e investigação de dissidentes políticos. Contudo, há um receio que a Convenção

[37] No original: “While the battle may have been won, the war is ongoing. Those concerning crimes may still find their way into the convention’s scope. Articles 61 and 62 provide that the Conference of the States Parties may supplement the convention with one or more additional protocols. These protocols only need to be submitted by at least 60 states, and while they should preferably be adopted by consensus, a two-thirds majority vote of the states parties present and voting would be enough to adopt them. This means that nothing prevents Russia or China, supported by 60 states, from proposing the adoption of a protocol that includes a provision against extremism-related offenses—opening the door for broad domestic interpretations.
The U.S. lead negotiator, Ambassador Deborah McCarthy, argued that it was a hard-fought victory for the U.S. team and its allies and partners to be able to set a high bar for the negotiation of a protocol, against constant opposition from more authoritarian-leaning states. It is true that Russia and China originally wanted fewer countries to be sufficient to bring about a protocol and to adopt it. It was, indeed, a compromise to raise the number to 60 states. But the option remains for not that many countries to unreasonably expand the scope of the convention and threaten fundamental freedoms. Articles 61 and 62 loom over fundamental freedoms and will require unwavering and continuous vigilance on the part of democratic states and civil society”.

de Hanói e seus eventuais protocolos adicionais sejam utilizados por Estados-Partes para atendimento desses interesses impróprios, o que esvaziaria parte de sua efetividade como instrumento a ser adotado internacionalmente, sobretudo ao se considerar as previsões de cooperação jurídica entre os Estados (Pavlova, 2025).

Por fim, não há como afirmar, por ora, que a Convenção de Budapeste e a Convenção da ONU serão harmônicas e complementares no enfrentamento de delitos, na cooperação jurídica internacional e na proteção de direitos humanos.

CONCLUSÃO

A análise comparativa entre a Convenção de Budapeste e a Convenção de Hanói permite concluir que ambos os instrumentos jurídicos são passos relevantes para o enfrentamento de cibercrimes, cujo caráter transfronteiriço exige dos Estados uma atuação alinhada e colaborativa na esfera internacional. O estudo demonstrou que, apesar de a Convenção de Budapeste ser um modelo em termos de proteção de direitos fundamentais, o seu alcance limitado e a percepção de ser um instrumento de matriz eurocêntrica impulsionaram a necessidade de um tratado de vocação universal sob a égide das Nações Unidas.

Contudo, a Convenção de Hanói, até o presente momento, não é capaz de presumir um alcance universal e nem a proteção de direitos humanos, com adequada cooperação jurídica internacional entre os países signatários. O exíguo rol de direitos fundamentais e a possibilidade de incrementos significativos por meio de protocolos adicionais, aprovados com quórum relativamente baixo, pode instrumentalizar o tratado para fins de vigilância política e repressão de dissidências.

Em última análise, rememorando Karine Bannelier e Eugenia Lostri (2024), a coexistência destes dois instrumentos exigirá uma vigilância contínua da sociedade civil e das democracias liberais. O desafio futuro não reside apenas na harmonização técnica das normas, mas na garantia de que o ciberespaço permaneça um ambiente seguro que não abdique das conquistas civilizacionais em prol de uma cooperação policial sem limites.

REFERÊNCIAS

BANNELIER, K. The U.N. cybercrime convention should not become a tool for political control or the watering down of human rights. **Lawfare**. Washington, 2023. Disponível em: https://www.lawfareblog.com/un-cybercrime-convention-should-not-become-tool-political-

control-or-watering-down-human-rights. Acesso em: 21 fev. 2023.

BANNELIER, K; LOSTRI, E. Is anyone happy with the UN Cybercrime Convention? **Lawfare**. Washington, 2024. Disponível em: https://www.lawfaremedia.org/article/is-anyone-happy-with-the-un-cybercrime-convention. Acesso em: 04 fev. 2026.

BARRETO, A. G.; KUFA, K.; SILVA, M. M. **Cibercrimes e seus reflexos no direito brasileiro**. 3. ed. rev., atual. e ampl. São Paulo: Juspodivm, 2022.

BECHARA, F. R. **Cooperação jurídica internacional em matéria penal**: eficácia da prova produzida no exterior. 2009. 198 f. Tese (Doutorado em Direito Processual) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2009.

BRITO, A. **Direito penal informático**. São Paulo: Saraiva, 2013.

CHANG, L. Y. Criminological perspectives on cybercrime: risk, routine activity, and cybercrime. **Research handbook on transnational crime**. Cheltenham: Edward Elgar, 2019. p. 327-355.

CHAWKI, M. et al. **Cybercrime, digital forensics and jurisdiction**. Cham: Springer, 2015. (Studies in Computational Intelligence, 593).

CLOUGH, J. **Principles of Cybercrime**. New York: Cambridge University Press, 2010.

CLOUGH, J. The Council of Europe Convention on Cybercrime: defining "crime" in a digital world. **Criminal Law Forum**, n. 23, p. 363-391, 2012.

COUNCIL OF EUROPE. **Convention on Cybercrime**. Budapest, 2001. Disponível em: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Acesso em: 21 fev. 2023.

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 23/2025 on the two Proposals for Council Decisions on the signing and conclusion of the United Nations Convention against Cybercrime.** Bruxelas, 2025. Disponível em: https://www.edps.europa.eu/system/files/2025-09/25-09-04_opinion_united_nations_convention_against_cybercrime_en.pdf. Acesso em: 04 fev. 2026.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002.

MAURER, T. **Cyber norm emergence at the United Nations**: an analysis of the activities at the UN regarding cyber-security. Cambridge: Belfer Center for Science and International Affairs, 2011. (Explorations in Cyber International Relations Discussion Paper Series, n. 11).

MÜLLER, I. **Cooperação jurídica internacional em matéria penal e seus reflexos no direito à prova no processo penal brasileiro**. 2013. 210 f. Tese (Doutorado em Direito Processual) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2013.

NORTON LIFELOCK INC. **Cyber Safety Insights Report**: Global Report. Tempe: Harris Insights & Analitics LLC, 2022. Disponível em: https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-online-creeping/. Acesso em: 21 fev. 2023.

PAVLOVA, P. **The Promise and Peril of the U.N. Convention Against Cybercrime.** Just Security, Reiss Center on Law and Security at New York University School of Law: Nova Iorque, 2025. Disponível em: https://www.justsecurity.org/124057/promise-peril-cybercrime-convention/. Acesso em: 04 fev. 2026.

STRADNER, I.; HESTER, E. **The UN Cybercrime Treaty**: A Trojan Horse for Suppressing Dissent. Foundation for Defense of Democracies. Washington, 2025. Disponível em: https://www.fdd.org/analysis/2025/10/23/the-un-cybercrime-treaty-a-trojan-horse-for-suppressing-dissent/. Acesso em: 04 fev. 2026.

UNITED KINGDOM. Home Department by Command of Her Majesty. **Serious and Organised Crime Strategy**. London, 2013. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf. Acesso em: 21 fev. 2023.

UNITED NATIONS. *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. **Note by the Secretariat A/AC.291/4**: Compilation of views submitted by Member States on the scope, objectives and structure (elements) of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. Viena, 2021. Disponível em: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html. Acesso em: 21 fev. 2023.

UNITED NATIONS. *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. **Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes**. Viena, 2023a. Disponível em: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf. Acesso em: 21 fev. 2023.

UNITED NATIONS. *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. **Note by the Chair A/AC.291/19**: Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. Viena, 2023b. Disponível em: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/2228246E_Advance_Copy.pdf. Acesso em: 21 fev. 2023.

UNITED NATIONS. *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. **Road map and mode of work for the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes**. Viena, 2022. Disponível em: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/AHC_Road_map.pd

f. Acesso em: 21 fev. 2023.

UNITED NATIONS. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. Hanoi, 2025. Disponível em: https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

UNITED NATIONS. General Assembly. **Report of the Secretary-General A/74/130**: Countering the use of information and communications technologies for criminal purposes. New York, 2019a. Disponível em: https://undocs.org/Home/Mobile?FinalSymbol=A%2F74%2F130&Language=E&DeviceType=Desktop&LangRequested=False. Acesso em: 21 fev. 2023.

UNITED NATIONS. General Assembly. **Resolution A/RES/74/247**: Countering the use of information and communications technologies for criminal purposes. New York, 2019b. Disponível em: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRes%2F74%2F247&Language=E&DeviceType=Desktop&LangRequested=False. Acesso em: 21 fev. 2023.

URBAS, G. Legal perspectives on cybercrime. In: MITSILEGAS, V. et al. (eds.). **Research Handbook on Transnational Crime**. Cheltenham: Edward Elgar, 2019, p. 316-326.