REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

A COOPERAÇÃO INTERNACIONAL NO COMBATE AOS CRIMES CIBERNÉTICOS

INTERNATIONAL COOPERATION IN COMBATING CYBERCRIME

Ciências Sociais Aplicadas • 27/08/2026

REGISTRO DOI: 10.70773/revistatopicos/787808182

Camila Dantas Rocha de Araújo[1]

Piero Matos de Gomes[2]

João Paulo Ribeiro de Mello Guimarães[3]

Leonardo Tuffi Hassan Arruda[4]

RESUMO

Os crimes cibernéticos apresentam alcance transnacional, rapidez de execução e capacidade de produzir danos em diferentes países a partir de uma única operação. A infraestrutura empregada pelos autores, os dados necessários à investigação, as instituições atingidas e as vítimas podem estar localizados em jurisdições distintas, o que reduz a eficácia de respostas exclusivamente nacionais. Este artigo analisa o papel da cooperação internacional na prevenção, investigação e repressão dos crimes cibernéticos, com atenção aos mecanismos de preservação e compartilhamento de provas digitais, à harmonização legislativa, à assistência jurídica mútua, à atuação de organismos policiais e aos limites impostos pela soberania e pelos direitos fundamentais. A pesquisa possui abordagem qualitativa, natureza bibliográfica e documental e caráter descritivo e analítico. Foram examinados trabalhos científicos, legislação brasileira, tratados internacionais e documentos produzidos por organismos especializados. Os resultados indicam que a cooperação internacional permite reduzir obstáculos relacionados à territorialidade, à volatilidade dos dados e à diversidade dos sistemas jurídicos. Entretanto, sua efetividade depende da existência de autoridades especializadas, canais permanentes de comunicação, procedimentos céleres, compatibilidade normativa e salvaguardas relacionadas à privacidade, à proteção de dados e ao devido processo legal. Conclui-se que o enfrentamento dos crimes cibernéticos requer um modelo cooperativo que concilie agilidade investigativa, soberania estatal e proteção dos direitos humanos.

Palavras-chave: Crimes Cibernéticos; Cooperação Internacional; Prova Digital; Convenção De Budapeste; Segurança Cibernética.

ABSTRACT

Cybercrime has a transnational reach, rapid execution and the capacity to cause harm in different countries through a single operation. The infrastructure used by offenders, the data required for investigations, the institutions affected and the victims may be located in different jurisdictions, reducing the effectiveness of exclusively national responses. This article analyzes the role of international cooperation in the prevention, investigation and prosecution of cybercrime, with attention to mechanisms for preserving and sharing digital evidence, legislative harmonization, mutual legal assistance, the activities of police organizations and the limits imposed by sovereignty and fundamental rights. The research adopts a qualitative approach and is bibliographic and documentary in nature, with descriptive and analytical characteristics. Scientific studies, Brazilian legislation, international treaties and documents produced by specialized organizations were examined. The results indicate that international cooperation helps reduce obstacles related to territoriality, data volatility and differences among legal systems. However, its effectiveness depends on specialized authorities, permanent communication channels, timely procedures, regulatory compatibility and safeguards related to privacy, data protection and due process. It is concluded that combating cybercrime requires a cooperative model capable of reconciling investigative efficiency, state sovereignty and the protection of human rights.

Keywords: Cybercrime; International Cooperation; Digital Evidence; Budapest Convention; Cybersecurity.

INTRODUÇÃO

A incorporação das tecnologias digitais às atividades econômicas, administrativas e sociais alterou as condições em que os delitos são planejados, executados e investigados. Sistemas bancários, serviços públicos, hospitais, empresas, instituições educacionais e infraestruturas essenciais passaram a depender de redes conectadas e bancos de dados. Essa dependência ampliou a eficiência de inúmeros serviços, mas também ofereceu novas oportunidades para fraudes, invasões, extorsões, furtos de informações, interrupções de sistemas e outras práticas ilícitas. O crime cibernético deixou de representar uma atividade restrita a agentes isolados e passou a integrar estruturas organizadas que atuam em mercados ilícitos especializados.

A expressão “crime cibernético”, abrange condutas distintas. Algumas dependem necessariamente de computadores e redes, como o acesso não autorizado, a interferência em sistemas, a disseminação de programas maliciosos e os ataques de indisponibilidade. Outras correspondem a infrações já conhecidas, mas ampliadas pela utilização das tecnologias, como estelionato, extorsão, falsidade, perseguição, exploração sexual, lavagem de dinheiro e violação de propriedade intelectual. Clough (2015) explica que a diversidade dessas condutas dificulta a elaboração de uma definição única, pois os recursos digitais podem aparecer como alvo, instrumento, ambiente ou meio de produção de provas.

Brenner (2010) observa que a estrutura descentralizada da Internet reduz a correspondência tradicional entre a localização do autor, o lugar da conduta e o território em que o resultado é produzido. Um agente pode acessar um sistema localizado em outro continente, utilizar servidores instalados em diferentes países, movimentar valores por diversas contas e atingir vítimas que não compartilham a

mesma jurisdição. Essa dispersão transforma um único episódio em objeto potencial de vários ordenamentos jurídicos.

A dimensão transnacional não está presente apenas nos ataques de grande repercussão. Fraudes realizadas por mensagens, invasões de contas, extorsões digitais e furtos de credenciais podem envolver plataformas estrangeiras, serviços de armazenamento em nuvem e empresas sediadas fora do território da vítima. Mesmo quando autor e vítima estão no mesmo país, os registros necessários à investigação podem estar sob o controle de uma empresa estrangeira ou distribuídos em centros de dados localizados em diferentes Estados.

Casino et al. (2022) assinalam que as provas digitais passaram a ocupar lugar relevante em quase todas as investigações criminais. Mensagens, dados cadastrais, endereços de protocolo de Internet, registros de conexão, arquivos armazenados, históricos de localização e informações sobre transações podem esclarecer fatos praticados dentro e fora do ambiente virtual. A presença de dados em outra jurisdição, porém, exige procedimentos compatíveis com a legislação do país que receberá o pedido e com as regras do Estado responsável pela investigação.

A volatilidade constitui uma característica decisiva da prova digital. Registros podem ser apagados automaticamente, contas podem ser desativadas, dados podem ser transferidos e endereços eletrônicos podem ser alterados em curto espaço de tempo. Procedimentos diplomáticos ou judiciais excessivamente demorados podem tornar a prova indisponível antes de sua obtenção. Brenner e Schwerha (2002) já apontavam que a investigação transnacional de delitos

informáticos exigia mecanismos capazes de preservar elementos probatórios sem eliminar as garantias processuais.

A cooperação internacional surge como resposta à diferença entre a circulação global dos dados e a competência territorial das autoridades. Um órgão policial não pode exercer livremente poderes de busca, apreensão ou interceptação no território de outro Estado. A execução de medidas investigativas fora das fronteiras nacionais depende, em regra, da atuação da autoridade competente do país solicitado ou de procedimentos previamente estabelecidos em tratados.

Os mecanismos tradicionais de cooperação incluem cartas rogatórias, pedidos de assistência jurídica mútua, extradição, transferência de processos, compartilhamento de informações policiais e formação de equipes conjuntas. Embora esses instrumentos também sejam utilizados em crimes convencionais, as características das provas digitais exigem procedimentos mais rápidos, canais especializados e capacidade técnica para compreender solicitações relacionadas a redes, dispositivos e provedores.

A cooperação não se limita à entrega de provas. Ela compreende a aproximação entre legislações, a capacitação de autoridades, o compartilhamento de informações sobre ameaças, a realização de operações coordenadas, a localização de ativos, a identificação de suspeitos e a proteção das vítimas. Interpol (2022) organiza sua estratégia global em torno da compreensão das ameaças, da coordenação de atividades operacionais transnacionais, do desenvolvimento de capacidades nacionais e da construção de parcerias entre autoridades públicas e instituições privadas.

Europol (2025) identifica que os dados se tornaram objeto, instrumento e mercadoria da economia do crime digital. Credenciais, documentos, informações financeiras e acessos a sistemas são obtidos, comercializados e empregados em diferentes modalidades delitivas. Essa cadeia pode reunir grupos responsáveis por localizar vulnerabilidades, vender acessos, desenvolver programas maliciosos, negociar pagamentos e ocultar os recursos obtidos. A fragmentação das tarefas dificulta a identificação de todos os participantes e amplia a necessidade de investigações coordenadas.

A Convenção sobre o Crime Cibernético, adotada em Budapeste em 2001, constituiu o primeiro tratado internacional voltado à harmonização de infrações, à definição de poderes processuais e à cooperação em matéria de crimes cibernéticos e provas eletrônicas. Embora tenha sido elaborada no âmbito do Conselho da Europa, sua adesão foi aberta a países de outras regiões. Em julho de 2026, a Convenção reunia 82 Estados Partes, entre eles o Brasil.

O Brasil depositou o instrumento de adesão em 30 de novembro de 2022. A Convenção entrou em vigor para o país no plano internacional em 1º de março de 2023 e foi promulgada pelo Decreto nº 11.491, de 12 de abril de 2023. A incorporação do tratado ampliou a participação brasileira na rede de cooperação formada por autoridades especializadas e estabeleceu referências para a preservação e obtenção de dados eletrônicos.

A evolução das plataformas digitais e do armazenamento em nuvem expôs limitações dos mecanismos originais. O Segundo Protocolo Adicional à Convenção de Budapeste, aberto à assinatura em 2022, introduziu formas ampliadas de cooperação para a

divulgação de informações cadastrais, dados sobre registros de nomes de domínio, situações emergenciais, videoconferências e investigações conjuntas. Spiezia (2022) considera que o protocolo procura reduzir a distância entre a velocidade de desaparecimento das provas e o tempo necessário à execução dos pedidos tradicionais.

A busca por um instrumento de alcance universal resultou na Convenção das Nações Unidas contra o Crime Cibernético, adotada pela Assembleia Geral em 24 de dezembro de 2024. O documento foi aberto à assinatura em Hanói, em outubro de 2025, e permaneceu disponível para assinatura na sede das Nações Unidas. Em 22 de julho de 2026, o tratado contava com 79 signatários e três Estados Partes, mas ainda não havia alcançado as quarenta ratificações necessárias para sua entrada em vigor. O Brasil assinou a Convenção em 25 de outubro de 2025.

A nova convenção amplia a possibilidade de cooperação para o compartilhamento de provas eletrônicas relacionadas a infrações graves, inclusive quando os fatos investigados não correspondem exclusivamente a crimes contra sistemas informáticos. Essa amplitude pode facilitar investigações transnacionais, mas também suscita questionamentos sobre privacidade, vigilância, liberdade de expressão, dupla incriminação e utilização de pedidos para finalidades incompatíveis com os direitos humanos.

A cooperação internacional precisa conciliar interesses que nem sempre se apresentam de forma harmônica. As autoridades necessitam de agilidade para preservar informações, identificar suspeitos e evitar novos danos. Ao mesmo tempo, a entrega de dados pessoais a governos estrangeiros pode afetar a privacidade, o

sigilo das comunicações e o direito de defesa. Ruohonen (2023) observa que os mecanismos recentes de acesso transfronteiriço procuram reduzir atrasos, mas criam debates sobre extraterritorialidade, proteção de dados e controle judicial.

A diversidade legislativa representa outro obstáculo. Uma conduta considerada criminosa em determinado país pode não possuir tipificação equivalente em outro. Também existem diferenças quanto ao grau de proteção das comunicações, aos requisitos para quebra de sigilo, aos períodos de retenção de registros e à responsabilidade dos provedores. A ausência de compatibilidade pode impedir a execução de um pedido ou comprometer a validade da prova produzida.

O problema de pesquisa que orienta este artigo é o seguinte: de que maneira a cooperação internacional pode tornar mais efetivo o combate aos crimes cibernéticos sem afastar a soberania dos Estados e a proteção dos direitos fundamentais? O objetivo geral consiste em analisar a importância dos instrumentos internacionais para a prevenção, investigação e repressão das infrações praticadas contra ou por meio de sistemas digitais.

Como objetivos específicos, pretende-se examinar a dimensão transnacional dos crimes cibernéticos, compreender os obstáculos relacionados à jurisdição e à obtenção de provas digitais, analisar os mecanismos previstos na Convenção de Budapeste e na Convenção das Nações Unidas e discutir os desafios da participação brasileira na cooperação internacional. Também se busca identificar condições institucionais necessárias para que os acordos produzam resultados concretos.

A relevância do estudo está associada à impossibilidade de enfrentar redes criminosas globais apenas com medidas internas. Leis nacionais continuam indispensáveis para tipificar condutas e autorizar procedimentos investigativos. Contudo, tornam-se insuficientes quando os autores, os recursos tecnológicos, os dados e os produtos do crime se encontram distribuídos por diferentes países. A resposta precisa alcançar a mesma dimensão transnacional utilizada pelos agentes criminosos.

METODOLOGIA

O estudo possui abordagem qualitativa, natureza bibliográfica e documental e objetivos descritivos e analíticos. A pesquisa qualitativa foi escolhida porque o problema envolve a interpretação de normas, conceitos jurídicos, tratados internacionais e documentos institucionais. Não se pretendeu medir a incidência estatística dos crimes cibernéticos, mas compreender como os instrumentos de cooperação enfrentam os obstáculos decorrentes da territorialidade, da volatilidade das provas e da diversidade legislativa.

A pesquisa bibliográfica foi desenvolvida a partir de livros e artigos científicos relacionados aos crimes cibernéticos, à jurisdição na Internet, à prova digital, à assistência jurídica mútua e à cooperação policial. Gil (2022) explica que a pesquisa bibliográfica permite analisar um problema por meio de conhecimentos já publicados, possibilitando comparar interpretações e identificar questões ainda não resolvidas.

As buscas foram realizadas em bases e repositórios acadêmicos, entre eles o Portal de Periódicos da Coordenação de

Aperfeiçoamento de Pessoal de Nível Superior, a Scientific Electronic Library Online, Oxford Academic, Cambridge Core e repositórios institucionais. Foram empregados os descritores “crime cibernético”, “cooperação internacional”, “prova digital”, “jurisdição digital”, “assistência jurídica mútua”, “Convenção de Budapeste” e “investigação transnacional”. Também foram utilizados os termos correspondentes em inglês e espanhol.

A etapa documental compreendeu a análise da Convenção sobre o Crime Cibernético, do Segundo Protocolo Adicional à Convenção de Budapeste, da Convenção das Nações Unidas contra o Crime Cibernético e de relatórios elaborados pelo Conselho da Europa, pelo Escritório das Nações Unidas sobre Drogas e Crime, pela Interpol e pela Europol. Também foram examinadas normas brasileiras relacionadas à cooperação penal, à Internet, à proteção de dados e à segurança cibernética.

O recorte temporal priorizou publicações produzidas entre 2015 e julho de 2026. Foram admitidas obras anteriores quando apresentavam contribuições reconhecidas para a delimitação dos crimes cibernéticos ou para a análise da cooperação transnacional. Essa escolha permitiu combinar trabalhos clássicos com documentos recentes, especialmente aqueles relacionados à entrada do Brasil na Convenção de Budapeste e à adoção da nova convenção das Nações Unidas.

Foram incluídas fontes com autoria identificada, relação direta com o problema e informações editoriais verificáveis. Excluíram-se conteúdos publicitários, textos sem fundamentação, documentos repetidos e publicações que tratavam apenas de medidas técnicas

de segurança, sem relação com investigação criminal ou cooperação jurídica.

O corpus foi organizado em seis categorias de análise: transnacionalidade dos delitos; conflitos de jurisdição; preservação e compartilhamento de provas digitais; assistência jurídica mútua; cooperação policial e judicial; e proteção de direitos fundamentais. A análise seguiu procedimentos de leitura, fichamento e comparação temática. Bardin (2016) explica que a análise de conteúdo permite reunir elementos recorrentes e interpretar relações entre diferentes documentos.

A pesquisa não envolveu participantes, entrevistas, questionários ou utilização de dados pessoais. Por esse motivo, não houve necessidade de submissão a comitê de ética em pesquisa. Foram observados os princípios de integridade acadêmica, identificação das fontes e fidelidade às ideias consultadas.

Entre as limitações estão a rápida modificação das tecnologias, o caráter recente de alguns tratados e a ausência de dados públicos uniformes sobre pedidos internacionais de cooperação. A Convenção das Nações Unidas ainda não estava em vigor durante a elaboração do estudo, o que impediu a análise de resultados práticos de sua aplicação. As conclusões possuem natureza bibliográfica e documental e não substituem estudos empíricos sobre investigações específicas.

DESENVOLVIMENTO

A Dimensão Transnacional dos Crimes Cibernéticos

A investigação criminal foi tradicionalmente estruturada a partir de referências territoriais. A autoridade policial atua dentro de determinada circunscrição, o juiz exerce jurisdição em espaço definido e a legislação penal estabelece critérios relacionados ao lugar da conduta ou do resultado. No ambiente digital, essas referências permanecem juridicamente importantes, mas são insuficientes para representar a trajetória dos dados e a distribuição dos participantes.

Svantesson (2017) sustenta que a aplicação automática de concepções territoriais ao ambiente digital produz conflitos de jurisdição. Um conteúdo pode ser criado em um país, armazenado em outro e acessado simultaneamente em muitos territórios. A simples possibilidade de acesso não deveria, por si só, autorizar todos os Estados a exercer jurisdição, pois essa interpretação permitiria pretensões ilimitadas e incompatíveis.

Os crimes cibernéticos podem atingir múltiplas vítimas por meio de uma única estrutura automatizada. Programas maliciosos são capazes de percorrer redes, explorar vulnerabilidades e comprometer dispositivos sem que o autor tenha contato direto com cada pessoa atingida. Em esquemas de fraude, mensagens podem ser enviadas em larga escala e adaptadas a diferentes idiomas, instituições e perfis sociais.

A organização do crime digital também se tornou especializada. Alguns agentes desenvolvem ferramentas, enquanto outros comercializam acessos, alugam estruturas, recrutam operadores, convertem valores ou negociam dados furtados. Europol (2024) identifica que ransomware, fraudes eletrônicas e exploração sexual permanecem entre as manifestações mais ameaçadoras do crime

praticado pela Internet, com grupos situados tanto dentro quanto fora dos territórios atingidos.

O modelo denominado crime como serviço permite que indivíduos sem elevado conhecimento técnico adquiram recursos prontos para a prática delitiva. Programas maliciosos, hospedagens protegidas, bases de credenciais e serviços de lavagem de ativos podem ser negociados em ambientes digitais restritos. Essa estrutura amplia o número de participantes e dificulta a atribuição individual das condutas.

A utilização de moedas virtuais e meios de pagamento digitais acrescenta uma camada financeira à investigação. Embora determinadas redes registrem publicamente as transações, a identificação dos responsáveis pode exigir informações mantidas por plataformas sediadas em diferentes países. A localização e o bloqueio de ativos dependem da cooperação entre autoridades, instituições financeiras e empresas de tecnologia.

A infraestrutura tecnológica também pode ser distribuída intencionalmente. Servidores são transferidos, domínios são registrados com dados falsos e conexões são roteadas por diversos países. Essa dispersão busca dificultar a identificação da origem e criar obstáculos jurídicos para as autoridades responsáveis pela investigação.

Interpol (2022) reconhece que um ataque pode reunir autores localizados em vários países, infraestrutura hospedada em diferentes jurisdições e vítimas distribuídas mundialmente. A instituição destaca que a resposta precisa ser coordenada porque nenhum

órgão nacional consegue reunir sozinho todas as informações necessárias.

A transnacionalidade não elimina a necessidade de atuação nacional. A investigação começa, em muitos casos, com a comunicação realizada pela vítima à autoridade local. O registro inicial, a preservação dos dispositivos, a coleta de documentos e a identificação dos prejuízos dependem de estruturas nacionais. A cooperação amplia essa atuação quando os elementos ultrapassam as fronteiras.

A efetividade da resposta depende da capacidade de identificar rapidamente quais países, empresas e autoridades possuem relação com os dados. Solicitações enviadas ao destinatário inadequado geram atrasos e podem permitir a exclusão dos registros. Diretórios atualizados, pontos de contato permanentes e equipes especializadas reduzem esse risco.

Jurisdição, Soberania e Aplicação da Lei Penal

A jurisdição corresponde ao poder de um Estado de elaborar normas, julgar conflitos e executar decisões. No campo penal, a territorialidade permanece como critério central, mas pode ser complementada por princípios relacionados à nacionalidade do autor, à nacionalidade da vítima, à proteção de interesses estatais e à repressão de condutas reconhecidas internacionalmente.

Clough (2015) explica que os delitos cibernéticos podem produzir reivindicações concorrentes. Diferentes Estados podem entender que possuem competência porque parte da conduta, da infraestrutura ou do resultado ocorreu em seus territórios. Essa sobreposição não é necessariamente ilegítima, mas precisa ser

administrada para evitar investigações duplicadas, decisões contraditórias e disputas sobre extradição.

A definição da jurisdição mais adequada pode considerar a localização predominante das vítimas, a residência do suspeito, a disponibilidade das provas, a gravidade dos resultados e a possibilidade de julgamento efetivo. A cooperação permite que autoridades compartilhem informações e decidam qual país apresenta melhores condições para conduzir o processo.

A soberania impede que um Estado execute atos coercitivos no território de outro sem autorização. Uma autoridade estrangeira não pode realizar busca física, apreender equipamentos ou impor obrigações diretamente a pessoas localizadas em outro país, salvo quando existir base jurídica aceita. A violação dessas regras pode comprometer relações diplomáticas e gerar questionamentos sobre a validade da prova.

O ambiente de nuvem torna a localização dos dados menos evidente. Uma empresa pode transferir informações automaticamente entre centros de processamento ou dividir arquivos em diferentes territórios. O investigador nem sempre sabe onde o conteúdo está armazenado no momento do pedido. Ruohonen (2023) afirma que essa realidade dificulta a utilização de regras baseadas exclusivamente no local físico do servidor.

Algumas propostas atribuem maior importância ao controle exercido pelo provedor sobre os dados. Nessa perspectiva, uma ordem poderia ser dirigida à empresa que possui capacidade de acesso, ainda que o conteúdo esteja armazenado em outro país. A solução acelera a obtenção, mas pode gerar conflitos quando o

cumprimento da ordem viola a legislação do território em que os dados se encontram.

A cooperação internacional procura evitar medidas unilaterais por meio de procedimentos reconhecidos. Tratados, acordos bilaterais e redes especializadas definem as condições em que as autoridades podem solicitar preservação, produção ou compartilhamento de informações. Esses instrumentos oferecem previsibilidade para os Estados e para as empresas responsáveis pelos dados.

A dupla incriminação constitui requisito presente em parte dos mecanismos. Ela exige que o fato investigado seja considerado ilícito tanto no país solicitante quanto no solicitado. O princípio protege a autonomia legislativa, mas pode dificultar a cooperação quando as tipificações possuem elementos diferentes ou quando uma conduta ainda não foi atualizada em um dos ordenamentos.

A harmonização legislativa reduz esse obstáculo. Ao estabelecer definições aproximadas de acesso ilícito, interceptação indevida, interferência em dados, interferência em sistemas e uso abusivo de dispositivos, a Convenção de Budapeste contribui para que os Estados reconheçam uma base comum. A harmonização não exige leis idênticas, mas busca assegurar equivalência suficiente para a cooperação.

A soberania não deve ser compreendida como isolamento. A adesão voluntária a tratados representa exercício da própria soberania, pois o Estado aceita obrigações e procedimentos para enfrentar problemas que não consegue solucionar isoladamente. O desafio consiste em garantir que a cooperação permaneça submetida à

legalidade, à reciprocidade e ao controle das instituições competentes.

A Convenção de Budapeste e a aproximação dos sistemas jurídicos

A Convenção de Budapeste foi aberta à assinatura em 23 de novembro de 2001. Sua estrutura combina direito penal material, medidas processuais e cooperação internacional. Essa organização reconhece que a existência de tipos penais não produz resultados quando as autoridades não possuem instrumentos para investigar e quando as provas dependem de outro país.

Na dimensão material, o tratado trata de condutas contra a confidencialidade, a integridade e a disponibilidade dos dados e sistemas. Também inclui falsidade e fraude informáticas, delitos relacionados a material de abuso sexual infantil e infrações de propriedade intelectual. Conselho da Europa (2001) propõe que cada Estado incorpore as condutas ao seu ordenamento de acordo com seus princípios jurídicos.

As medidas processuais abrangem preservação expedita de dados armazenados, apresentação de informações, busca e apreensão de dados, coleta em tempo real de dados de tráfego e interceptação de conteúdo. Essas medidas não se limitam aos delitos previstos na Convenção. Podem ser utilizadas para colher prova eletrônica de outras infrações, desde que respeitadas as condições estabelecidas pelo direito interno.

A preservação expedita ocupa posição relevante porque impede a exclusão dos dados enquanto o pedido formal é preparado. Ela não corresponde necessariamente à entrega imediata do conteúdo. O

provedor ou a autoridade responsável mantém os registros por determinado período, possibilitando que a solicitação posterior seja analisada segundo os requisitos legais.

A distinção entre preservação e divulgação protege simultaneamente a investigação e o devido processo. A primeira medida reduz o risco de desaparecimento da informação. A segunda permanece sujeita à autorização competente, especialmente quando envolve conteúdo de comunicações ou dados protegidos por sigilo.

A Convenção estabelece mecanismos de assistência jurídica mútua e prevê que as partes prestem cooperação na maior extensão possível. Também orienta os Estados a aceitar pedidos por meios rápidos quando a urgência justificar, com posterior confirmação pelos canais formais. A intenção é adaptar a cooperação à velocidade das provas eletrônicas.

O artigo 35 determina a criação de uma rede de pontos de contato disponíveis durante vinte e quatro horas por dia e sete dias por semana. Esses pontos oferecem assistência imediata, orientam pedidos, promovem preservação de dados e facilitam a comunicação entre as autoridades. Em 2026, a rede incluía o Brasil e era formada, em geral, por unidades policiais ou órgãos de persecução especializados.

A rede não substitui todos os procedimentos de assistência mútua. Sua função principal está relacionada à preservação, ao fornecimento de informações técnicas e à preparação de solicitações urgentes. Quando o dado preservado precisa ser

apresentado como prova, pode ser necessária uma etapa formal posterior.

Spiezia (2022) considera que o Segundo Protocolo Adicional procura responder ao aumento do armazenamento em nuvem e à presença global dos provedores. O documento prevê cooperação direta para determinadas categorias de informações, especialmente dados cadastrais, além de procedimentos para situações emergenciais e investigações conjuntas.

A obtenção direta de dados pode reduzir atrasos, mas deve observar as condições impostas pelo país e pelo protocolo. O nível de proteção varia conforme a natureza da informação. Dados de conteúdo recebem tratamento mais restritivo porque revelam o teor das comunicações e produzem maior interferência na vida privada.

O protocolo também estabelece salvaguardas de proteção de dados pessoais. Finalidade, proporcionalidade, segurança e limitação do tratamento aparecem como condições para a transmissão. A existência de regras específicas procura impedir que a cooperação seja utilizada como forma de contornar garantias nacionais.

A adesão brasileira fortaleceu a inserção do país em um sistema já utilizado por autoridades de diferentes regiões. O Conselho da Europa registrava 82 partes em julho de 2026, além de outros países signatários ou convidados a aderir. A quantidade de participantes amplia a possibilidade de utilização de procedimentos comuns em investigações que envolvam diferentes territórios.

Assistência Jurídica Mútua e Obtenção de Provas Digitais

A assistência jurídica mútua permite que um Estado solicite a outro a realização de atos necessários a uma investigação ou processo. Entre as medidas estão obtenção de documentos, identificação de pessoas, bloqueio de bens, busca, apreensão, oitiva de testemunhas e entrega de dados mantidos por empresas.

Os pedidos costumam ser encaminhados por autoridades centrais. Essas instituições verificam os requisitos formais, analisam a base jurídica e encaminham a solicitação ao órgão responsável pela execução. O procedimento oferece segurança jurídica, mas pode enfrentar demora quando o documento precisa percorrer várias etapas administrativas.

No caso das provas digitais, a demora possui consequências específicas. Determinados provedores conservam informações durante períodos limitados e podem apagar registros de acordo com suas políticas internas. A investigação precisa identificar rapidamente quais dados existem, quem os controla e qual procedimento deve ser utilizado.

Jerman Blažič e Klobučar (2020) observam que os mecanismos tradicionais nem sempre correspondem à velocidade dos fluxos eletrônicos. Os autores defendem procedimentos capazes de superar barreiras sem afastar a legalidade e o controle judicial. A simplificação precisa ser acompanhada por critérios claros sobre autoridade, finalidade e extensão da medida.

O pedido deve descrever os fatos investigados, a relação entre os dados e o crime, o período de interesse, a conta ou sistema envolvido e a medida solicitada. Pedidos genéricos podem ser

recusados por falta de proporcionalidade. A precisão também auxilia o provedor ou a autoridade estrangeira a localizar as informações.

A cadeia de custódia precisa ser preservada durante a transferência. A prova deve manter autenticidade, integridade e possibilidade de verificação. Registros de quem coletou, armazenou, copiou e enviou os arquivos são necessários para demonstrar que o conteúdo não foi alterado.

Casino et al. (2022) destacam que a diversidade dos procedimentos forenses e dos padrões jurídicos pode comprometer o compartilhamento. Um método aceito no país que coleta o dado pode ser questionado no processo em que ele será utilizado. Protocolos técnicos e documentação adequada reduzem esse problema.

A tradução constitui outra dificuldade. Termos técnicos podem não possuir correspondência direta e erros podem modificar o alcance da medida solicitada. Equipes com formação jurídica, linguística e tecnológica são mais adequadas para elaborar e interpretar pedidos.

A assistência também pode ser recusada quando o pedido afeta interesses essenciais, contraria a ordem pública, envolve discriminação ou não apresenta garantias suficientes. Tratados internacionais costumam prever motivos de recusa e possibilidades de consulta antes da decisão definitiva.

O princípio da especialidade limita o uso da prova à finalidade que justificou sua entrega. Caso a autoridade pretenda utilizar o material em outro processo, pode ser necessária autorização adicional. A regra impede que dados fornecidos para investigação específica sejam empregados de forma indiscriminada.

A presença de empresas privadas ocupa espaço central. Grande parte dos dados relevantes está sob controle de provedores de conexão, redes sociais, plataformas de armazenamento, instituições financeiras e serviços de comunicação. A cooperação estatal precisa dialogar com obrigações privadas de retenção, segurança e proteção dos usuários.

Empresas globais recebem pedidos de diferentes países e precisam avaliar sua compatibilidade com várias legislações. Formulários padronizados, canais autenticados e indicações claras da base jurídica facilitam o processamento. A informalidade excessiva, porém, pode comprometer a validade e a segurança da entrega.

Cooperação Policial, Redes Especializadas e Operações Conjuntas

A cooperação policial possibilita o intercâmbio de informações antes ou durante a investigação formal. Unidades especializadas podem compartilhar indicadores técnicos, identificar padrões, localizar suspeitos e coordenar medidas realizadas simultaneamente em diferentes países.

A Interpol não substitui as polícias nacionais nem exerce poder de prisão. Sua função consiste em facilitar a comunicação, organizar bases de dados, produzir análises e apoiar operações. Quando a coordenação internacional é necessária, as autoridades nacionais utilizam os canais da organização para compartilhar informações e articular medidas.

A Estratégia Global contra o Crime Cibernético 2022 a 2025 estabeleceu objetivos relacionados à análise de inteligência, interrupção de estruturas criminosas, capacitação e fortalecimento de parcerias. Interpol (2022) reconhece que a atuação precisa ser

orientada por informações compartilhadas e não apenas por respostas isoladas a incidentes concluídos.

A Europol desenvolve função semelhante no espaço europeu, oferecendo suporte analítico e operacional às autoridades nacionais. Seu Centro Europeu de Crimes Cibernéticos reúne conhecimentos especializados e participa de investigações contra programas maliciosos, fraudes, exploração sexual e estruturas de crime como serviço.

Operações conjuntas aumentam a possibilidade de apreender equipamentos, retirar serviços ilícitos do ar, bloquear ativos e prender suspeitos em curto intervalo. A coordenação temporal é necessária porque a realização de uma medida em um país pode alertar participantes localizados em outros territórios.

Equipes conjuntas de investigação permitem que representantes de diferentes Estados trabalhem de forma integrada. Elas podem compartilhar informações, planejar diligências e evitar a duplicação de esforços. Sua criação depende de base jurídica e definição das competências de cada participante.

As equipes também facilitam a escolha do país responsável pelo processo. Quando várias jurisdições possuem elementos relevantes, a análise conjunta pode considerar localização dos suspeitos, número de vítimas, disponibilidade das provas e possibilidade de reparação.

A cooperação policial não dispensa a cooperação judicial quando a medida restringe direitos. Informações abertas e elementos de inteligência podem circular por canais mais rápidos. Busca,

apreensão, interceptação e divulgação de conteúdo normalmente exigem autorização prevista na legislação competente.

Os centros de resposta a incidentes também contribuem para a prevenção e contenção. Embora não sejam órgãos de persecução, podem identificar ataques, compartilhar indicadores técnicos e orientar instituições atingidas. A integração entre resposta técnica e investigação criminal precisa respeitar atribuições e regras sobre sigilo.

Parcerias com o setor privado são necessárias porque empresas identificam comportamentos maliciosos, controlam infraestruturas e preservam registros. Entretanto, a cooperação não deve transferir às plataformas funções próprias do Estado nem permitir coleta indiscriminada de informações.

A confiança entre autoridades representa elemento prático de grande importância. Canais formais são indispensáveis, mas sua utilização se torna mais eficiente quando os profissionais conhecem os procedimentos e conseguem esclarecer dúvidas diretamente. Reuniões, treinamentos e exercícios conjuntos contribuem para essa confiança.

Países com menor capacidade técnica precisam receber formação e infraestrutura. Uma rede internacional se torna vulnerável quando parte dos participantes não consegue preservar dados, analisar dispositivos ou responder com segurança. A cooperação deve incluir redução das desigualdades institucionais entre os Estados.

A Convenção das Nações Unidas contra o Crime Cibernético

A criação de uma convenção no âmbito das Nações Unidas procurou estabelecer um instrumento de alcance global. A Convenção de Budapeste possui ampla participação, mas não reúne todos os Estados e foi objeto de críticas relacionadas à sua origem regional e às concepções de soberania digital.

A Convenção das Nações Unidas foi adotada pela Resolução nº 79/243, em 24 de dezembro de 2024. Seu título completo destaca duas finalidades: combater determinadas infrações cometidas por sistemas de informação e compartilhar provas eletrônicas relacionadas a crimes graves.

O documento possui nove capítulos, que tratam de disposições gerais, criminalização, jurisdição, medidas processuais, cooperação internacional, prevenção, assistência técnica, implementação e disposições finais. Escritório das Nações Unidas sobre Drogas e Crime (2024) afirma que o tratado procura oferecer uma estrutura comum para Estados com diferentes tradições jurídicas.

A Convenção prevê crimes relacionados ao acesso ilegal, à interceptação, à interferência em dados, à interferência em sistemas, ao uso indevido de dispositivos e à fraude. Também inclui disposições sobre exploração e abuso sexual infantil, compartilhamento não consentido de imagens íntimas e lavagem de produtos obtidos por meio das infrações.

As medidas processuais alcançam a coleta, obtenção, preservação e transmissão de provas eletrônicas. O tratado reconhece que esses dados podem ser relevantes para diversos crimes graves, ainda que a conduta investigada não tenha sido praticada diretamente contra um sistema informático.

A cooperação internacional inclui extradição, assistência jurídica mútua, transferência de processos, investigações conjuntas, recuperação de ativos e uma rede disponível permanentemente. A proposta busca reduzir diferenças entre países que já participam de outros acordos e Estados que ainda não dispõem de instrumentos específicos.

Em julho de 2026, a Convenção ainda não estava em vigor. O tratado necessitava de quarenta instrumentos de ratificação, aceitação, aprovação ou adesão. Naquela data, havia 79 signatários e apenas três partes. A assinatura demonstra intenção política, mas não substitui os procedimentos internos necessários à vinculação definitiva.

O Brasil participou das negociações e assinou o tratado em 25 de outubro de 2025. A futura ratificação exigirá avaliação de compatibilidade com a Constituição, com a legislação penal, com a Lei Geral de Proteção de Dados Pessoais e com as regras nacionais de cooperação.

A amplitude da Convenção constitui sua principal possibilidade e também seu ponto de tensão. Um instrumento global pode aproximar países que não compartilham outros tratados. Ao mesmo tempo, pedidos de dados podem partir de Estados com níveis distintos de proteção judicial, liberdade de expressão e privacidade.

As salvaguardas de direitos humanos precisam ser aplicadas em conjunto com as disposições de cooperação. A autoridade solicitada deve verificar se o pedido está relacionado a finalidade legítima, se a medida é proporcional e se existem riscos de perseguição, discriminação ou utilização incompatível com o devido processo.

A implementação nacional será decisiva. Um tratado não produz cooperação rápida apenas pela existência de normas. Estados precisam designar autoridades, criar procedimentos, formar profissionais, garantir segurança na comunicação e estabelecer critérios de controle.

A relação entre a Convenção das Nações Unidas e a Convenção de Budapeste não deve ser necessariamente compreendida como substituição. Os instrumentos podem coexistir. Países que integram ambos poderão escolher a base mais adequada, desde que preservem as garantias e evitem conflitos entre obrigações.

O Brasil e os Instrumentos Nacionais de Cooperação

A participação brasileira no combate internacional aos crimes cibernéticos envolve normas penais, processuais, digitais e diplomáticas. Antes da adesão à Convenção de Budapeste, o país já utilizava acordos bilaterais e multilaterais de assistência jurídica em matéria penal.

O Decreto nº 3.810, de 2 de maio de 2001, promulgou o acordo de assistência judiciária entre Brasil e Estados Unidos. O instrumento possui importância porque muitas empresas de tecnologia responsáveis por dados utilizados por brasileiros estão sediadas nos Estados Unidos.

O Decreto nº 6.340, de 3 de janeiro de 2008, promulgou a Convenção Interamericana sobre Assistência Mútua em Matéria Penal. O documento estabelece procedimentos de cooperação entre países do continente e permite a realização de atos necessários à investigação e ao processo.

O Marco Civil da Internet, instituído pela Lei nº 12.965, de 23 de abril de 2014, define princípios, garantias e deveres para o uso da Internet no Brasil. A norma disciplina a guarda de registros e estabelece condições para sua disponibilização, vinculando o acesso ao respeito à intimidade, à vida privada e ao controle judicial.

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018, estabelece princípios para o tratamento de informações pessoais. Embora sua aplicação às atividades de investigação possua regras próprias, finalidade, necessidade, segurança e responsabilização permanecem referências relevantes para a transmissão internacional de dados.

A adesão à Convenção de Budapeste foi concluída com a promulgação pelo Decreto nº 11.491/2023. O tratado passou a integrar o ordenamento brasileiro e criou novas possibilidades para a cooperação em crimes cibernéticos e provas eletrônicas.

A Política Nacional de Cibersegurança foi instituída pelo Decreto nº 11.856, de 26 de dezembro de 2023. Entre seus princípios estão soberania, proteção dos direitos fundamentais, prevenção de incidentes, resiliência e cooperação internacional. A política também criou o Comitê Nacional de Cibersegurança.

A Estratégia Nacional de Cibersegurança, instituída pelo Decreto nº 12.573, de 4 de agosto de 2025, organizou ações em quatro eixos: proteção do cidadão, segurança de serviços essenciais, cooperação entre instituições e soberania nacional. O documento inclui o combate aos crimes cibernéticos e a colaboração internacional entre seus objetivos.

A existência de normas não elimina problemas de coordenação. Polícia Federal, polícias estaduais, Ministério Público, Poder Judiciário, autoridades centrais e órgãos de segurança cibernética possuem funções diferentes. A efetividade depende de procedimentos que permitam identificar rapidamente qual instituição deve agir.

A formação profissional representa outra necessidade. A elaboração de um pedido de cooperação exige conhecimento do direito interno, do tratado aplicável, da legislação do país solicitado e das características técnicas do dado. Erros formais ou descrições imprecisas podem provocar recusas.

A descentralização federativa brasileira também precisa ser considerada. Muitos crimes são investigados pelas polícias civis e processados pela Justiça estadual, mas a cooperação internacional envolve autoridades federais e canais diplomáticos. Protocolos claros são necessários para que investigações locais acessem os instrumentos internacionais.

O atendimento às vítimas precisa fazer parte da estratégia. A cooperação costuma concentrar-se na identificação dos autores, mas também deve buscar interrupção do dano, recuperação de valores, retirada de conteúdos ilícitos e comunicação transparente sobre o andamento possível.

O Brasil possui capacidade técnica e jurídica para participar das redes internacionais, mas precisa ampliar estatísticas, formação e integração. Dados consistentes sobre pedidos enviados, pedidos recebidos, tempo de resposta e resultados ajudariam a avaliar a efetividade dos mecanismos.

Direitos Fundamentais e Limites da Cooperação

A necessidade de combater crimes graves não afasta a proteção da intimidade, da liberdade e do devido processo. A cooperação internacional amplia o número de instituições que podem acessar dados e torna mais complexa a identificação de responsabilidades.

A Constituição brasileira protege a intimidade, a vida privada e o sigilo das comunicações. Medidas de investigação precisam apresentar base legal, finalidade legítima e controle proporcional. A transferência internacional não reduz essas exigências.

O conteúdo de mensagens possui grau elevado de proteção. Informações cadastrais, dados de tráfego e conteúdo comunicacional não produzem a mesma interferência e podem receber procedimentos diferentes. A classificação precisa ser clara para impedir que categorias menos protegidas sejam utilizadas para revelar informações mais sensíveis.

A proporcionalidade exige relação entre a gravidade do fato e a extensão da medida. Pedidos abrangentes, sem delimitação temporal ou sem indicação do vínculo com o crime, podem atingir pessoas não investigadas e criar bancos de dados incompatíveis com a finalidade declarada.

A dupla incriminação oferece proteção contra pedidos baseados em condutas não reconhecidas como crime pelo Estado solicitado. Entretanto, sua aplicação precisa considerar equivalência material e não apenas identidade literal entre os tipos penais.

A possibilidade de recusa por motivos de direitos humanos também é necessária. Um Estado não deve fornecer dados quando existirem

razões concretas para acreditar que serão utilizados em perseguição política, discriminação ou aplicação de tratamento incompatível com a dignidade humana.

A liberdade de expressão merece atenção especial. Leis excessivamente amplas podem classificar críticas, pesquisas ou manifestações legítimas como crimes digitais. A cooperação não pode converter divergências políticas em fundamento para vigilância transnacional.

Pesquisadores de segurança identificam falhas e comunicam vulnerabilidades. A ausência de critérios sobre autorização e intenção pode aproximar atividades legítimas de tipos penais relacionados ao acesso indevido. Regras nacionais e internacionais precisam distinguir pesquisa responsável de condutas voltadas à obtenção de vantagem ou produção de dano.

A defesa deve ter possibilidade de questionar a origem, a integridade e a legalidade das provas estrangeiras. Documentos técnicos sobre coleta, preservação e transmissão precisam integrar o processo. A cooperação não pode impedir o contraditório.

Empresas também devem publicar informações sobre pedidos governamentais, respeitados os limites necessários às investigações. Relatórios de transparência permitem acompanhar o volume de solicitações e os critérios gerais de atendimento.

A proteção de dados requer medidas de segurança durante a transmissão. Canais inadequados podem expor informações sensíveis, comprometer investigações e gerar novos danos às vítimas. Autenticação, criptografia, registro de acesso e limitação de armazenamento são componentes da cooperação responsável.

A eficiência não deve ser medida apenas pelo número de dados entregues ou pela rapidez das respostas. Uma cooperação legítima precisa produzir provas utilizáveis, proteger pessoas inocentes e permitir responsabilização em caso de abuso.

RESULTADOS E DISCUSSÕES

A análise bibliográfica e documental identificou que a cooperação internacional não representa uma medida complementar, mas um elemento estrutural do enfrentamento aos crimes cibernéticos. A distribuição de autores, vítimas, servidores, empresas e recursos financeiros por diferentes territórios impede que uma única autoridade reúna todos os elementos necessários à investigação.

O primeiro resultado está relacionado à importância da harmonização legislativa. A existência de definições aproximadas reduz dúvidas sobre dupla incriminação e facilita a execução dos pedidos. A Convenção de Budapeste possui contribuição consolidada nesse aspecto ao combinar tipificação, medidas processuais e cooperação. A nova Convenção das Nações Unidas amplia o alcance geográfico, mas sua efetividade dependerá das ratificações e da implementação nacional.

O segundo resultado mostra que a preservação expedita é uma das medidas mais adequadas às características da prova digital. Ela oferece tempo para a preparação do pedido formal sem autorizar automaticamente a divulgação do conteúdo. A separação entre preservação e entrega permite conciliar urgência e controle jurídico.

O terceiro resultado indica que os canais permanentes de comunicação reduzem atrasos e erros. A rede prevista no artigo 35 da Convenção de Budapeste permite contato entre equipes

especializadas e oferece apoio imediato em investigações urgentes. Sua utilidade depende de disponibilidade real, conhecimento técnico e atualização das informações de contato.

O quarto resultado refere-se à insuficiência dos tratados quando as instituições nacionais não possuem recursos. Cooperação internacional exige unidades especializadas, equipamentos, peritos, tradutores e profissionais capazes de elaborar pedidos. Países com menor estrutura podem integrar formalmente os acordos, mas apresentar dificuldades para utilizá-los.

O quinto resultado demonstra que a cooperação policial e a cooperação judicial possuem funções complementares. A primeira favorece inteligência, identificação e coordenação operacional. A segunda oferece base para medidas coercitivas e produção de prova. A tentativa de substituir uma pela outra pode gerar ilegalidade ou demora.

O sexto resultado envolve a participação das empresas privadas. Provedores e plataformas controlam grande parte das informações necessárias, mas não devem definir sozinhos o equilíbrio entre investigação e privacidade. Tratados e leis precisam estabelecer obrigações, possibilidades de recusa e critérios de transparência.

A análise também revelou tensão entre rapidez e proteção de direitos. Procedimentos diretos podem evitar o desaparecimento dos registros, mas reduzem etapas nas quais autoridades nacionais verificariam a legalidade. Por isso, a simplificação precisa ser acompanhada por critérios de necessidade, proporcionalidade, finalidade e segurança.

Outro resultado está relacionado à coexistência de diferentes instrumentos. A Convenção de Budapeste, seus protocolos, acordos bilaterais, convenções regionais e a Convenção das Nações Unidas formam um conjunto que pode ampliar as possibilidades de cooperação. Entretanto, a multiplicidade também exige que as autoridades saibam escolher a base jurídica adequada.

No caso brasileiro, a adesão à Convenção de Budapeste, a Política Nacional de Cibersegurança e a Estratégia Nacional de Cibersegurança ampliaram a base institucional. Ainda permanecem desafios relacionados à integração federativa, à capacitação, à uniformização de procedimentos e à produção de indicadores públicos.

Os resultados confirmam a interpretação de Casino et al. (2022) de que a heterogeneidade jurídica representa um dos principais obstáculos às investigações transfronteiriças. Também se aproximam de Spiezia (2022), para quem os mecanismos recentes precisam reduzir o tempo de resposta sem enfraquecer a proteção das pessoas afetadas.

Como limitação, o estudo não analisou processos criminais concretos nem dados internos das autoridades centrais. Pesquisas futuras podem examinar o tempo médio dos pedidos, os motivos de recusa, a utilização da rede permanente e os efeitos da entrada do Brasil na Convenção de Budapeste.

CONSIDERAÇÕES FINAIS

Os crimes cibernéticos desafiam os modelos tradicionais de investigação porque suas etapas não permanecem limitadas ao território de um único Estado. Autores, vítimas, provedores,

servidores, dados e ativos podem estar distribuídos por diversas jurisdições. Essa característica permite que os agentes explorem diferenças legislativas e dificuldades de comunicação entre autoridades.

O artigo analisou como a cooperação internacional pode fortalecer o enfrentamento dessas práticas sem afastar a soberania e os direitos fundamentais. A pesquisa demonstrou que a resposta depende de uma combinação entre legislação nacional, tratados, redes policiais, autoridades centrais, unidades especializadas e participação regulada do setor privado.

A Convenção de Budapeste representa um marco porque reúne três dimensões que precisam permanecer articuladas. A primeira corresponde à aproximação das definições penais. A segunda oferece instrumentos processuais adequados às provas digitais. A terceira estabelece formas de cooperação e uma rede permanente de contato.

O Segundo Protocolo Adicional amplia as possibilidades de obtenção de informações em contextos marcados pelo armazenamento em nuvem e pela presença internacional dos provedores. Seus mecanismos podem reduzir o tempo necessário à identificação de contas, à preservação de registros e à resposta a situações emergenciais. Essa agilidade, porém, precisa ser acompanhada por salvaguardas de proteção de dados.

A Convenção das Nações Unidas apresenta possibilidade de maior abrangência geográfica. Sua adoção demonstra reconhecimento de que o problema não pode ser solucionado por acordos limitados a determinados grupos de países. Entretanto, o documento ainda não

estava em vigor em julho de 2026, e sua aplicação dependerá das ratificações e da capacidade institucional dos futuros Estados Partes.

A coexistência dos dois sistemas pode fortalecer a cooperação. A Convenção de Budapeste possui experiência acumulada e redes operacionais consolidadas. A Convenção das Nações Unidas pode aproximar países que não participam do primeiro instrumento. O uso complementar deve evitar redução das garantias já existentes.

A obtenção de provas digitais permanece como ponto central. Dados podem ser apagados rapidamente e transferidos entre diferentes estruturas. A preservação expedita oferece solução adequada porque impede a perda da informação sem autorizar automaticamente seu acesso.

A assistência jurídica mútua continua necessária para medidas que exigem controle formal. Sua modernização depende de formulários padronizados, comunicação eletrônica segura, autoridades especializadas e prazos compatíveis com a natureza dos dados. A eliminação indiscriminada de etapas não representa solução adequada.

A cooperação policial contribui para a produção de inteligência, localização de suspeitos e planejamento de operações conjuntas. Interpol, Europol e redes regionais ampliam a capacidade de identificar vínculos que não seriam percebidos em investigações isoladas. A informação policial precisa ser convertida em prova de acordo com os requisitos processuais.

A atuação das empresas de tecnologia deve ser regulada. Elas possuem dados e capacidade técnica, mas não podem substituir o controle judicial nem definir unilateralmente as condições de

investigação. Obrigações claras protegem os usuários e oferecem segurança jurídica para o atendimento das solicitações.

A soberania permanece relevante. Cada Estado conserva a responsabilidade de proteger as pessoas sob sua jurisdição e de impedir medidas coercitivas estrangeiras não autorizadas. A cooperação baseada em tratados não elimina a soberania, mas estabelece formas consentidas de exercício coordenado.

Os direitos fundamentais precisam orientar todas as etapas. Privacidade, proteção de dados, liberdade de expressão, contraditório e devido processo não constituem obstáculos externos à investigação. Eles são condições de legitimidade e contribuem para que a prova obtida seja válida e confiável.

Pedidos internacionais devem apresentar finalidade definida, relação com o fato investigado e delimitação do período e das informações. A coleta excessiva aumenta riscos para pessoas não envolvidas e pode provocar recusa do Estado solicitado. Precisão e proporcionalidade melhoram a eficácia.

O Brasil avançou com a adesão à Convenção de Budapeste, a instituição da Política Nacional de Cibersegurança e a atualização da Estratégia Nacional de Cibersegurança. O país também assinou a Convenção das Nações Unidas em 2025. Esses atos ampliam sua participação, mas não garantem resultados sem implementação.

A implementação brasileira requer integração entre órgãos federais e estaduais. Delegacias locais precisam conhecer os canais disponíveis e receber apoio para elaborar pedidos. Autoridades centrais devem dispor de equipes suficientes para processar solicitações nacionais e estrangeiras.

A formação precisa reunir direito, tecnologia e cooperação internacional. O investigador deve compreender os dados solicitados, enquanto o profissional responsável pela cooperação precisa conhecer as exigências jurídicas e técnicas. A ausência dessa integração produz pedidos incompletos e perda de tempo.

Também é necessário aperfeiçoar estatísticas. A publicação de dados agregados sobre solicitações, respostas, prazos e resultados permitiria avaliar gargalos e planejar investimentos. Transparência institucional não significa divulgar informações sigilosas de investigações, mas oferecer indicadores sobre o funcionamento do sistema.

A cooperação deve incluir apoio às vítimas. Interromper ataques, retirar conteúdos, recuperar valores e orientar instituições atingidas são medidas tão relevantes quanto a punição dos autores. Uma abordagem centrada apenas na persecução pode deixar os danos sem resposta adequada.

Conclui-se que a cooperação internacional é indispensável ao combate aos crimes cibernéticos, mas não deve ser entendida como simples circulação de dados entre governos. Trata-se de um sistema que precisa combinar confiança, rapidez, capacidade técnica, controle jurídico e proteção dos direitos humanos.

A resposta será efetiva quando conseguir acompanhar a velocidade dos delitos sem reproduzir práticas de vigilância incompatíveis com a democracia. O objetivo não consiste em permitir acesso ilimitado às informações, mas garantir que dados necessários sejam preservados e obtidos por procedimentos legítimos, seguros e proporcionais.

REFERÊNCIAS BIBLIOGRÁFICAS

BARDIN, Laurence. **Análise de conteúdo.** São Paulo: Edições 70, 2016.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023.** Promulga a Convenção sobre o Crime Cibernético, firmada em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023.** Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023.

BRASIL. **Decreto nº 12.573, de 4 de agosto de 2025.** Institui a Estratégia Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2025.

BRASIL. **Decreto nº 3.810, de 2 de maio de 2001.** Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América. Brasília, DF: Presidência da República, 2001.

BRASIL. **Decreto nº 6.340, de 3 de janeiro de 2008.** Promulga a Convenção Interamericana sobre Assistência Mútua em Matéria Penal. Brasília, DF: Presidência da República, 2008.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República,

2018.

BRENNER, Susan W. **Cybercrime: criminal threats from cyberspace.** Santa Barbara: Praeger, 2010.

BRENNER, Susan W.; SCHWERHA, Joseph J. Transnational evidence gathering and local prosecution of international cybercrime. **Journal of Computer & Information Law,** Chicago, v. 20, n. 3, p. 347-395, 2002.

CASINO, Fran et al. SoK: cross-border criminal investigations and digital evidence. **Journal of Cybersecurity,** Oxford, v. 8, n. 1, art. tyac014, 2022. DOI: 10.1093/cybsec/tyac014.

CLOUGH, Jonathan. **Principles of cybercrime.** 2. ed. Cambridge: Cambridge University Press, 2015. DOI: 10.1017/CBO9781139540803.

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

CONSELHO DA EUROPA. **Segundo Protocolo Adicional à Convenção sobre o Crime Cibernético relativo ao reforço da cooperação e à divulgação de provas eletrônicas.** Estrasburgo: Conselho da Europa, 2022.

EUROPOL. **Internet organised crime threat assessment 2024.** The Hague: European Union Agency for Law Enforcement Cooperation, 2024.

EUROPOL. **Steal, deal and repeat: how cybercriminals trade and exploit your data.** Luxembourg: Publications Office of the European Union, 2025. DOI: 10.2813/4926508.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 7. ed. São Paulo: Atlas, 2022.

INTERPOL. **Cybercrime global strategy 2022-2025.** Lyon: International Criminal Police Organization, 2022.

INTERPOL. **National cybercrime strategy guidebook.** Lyon: International Criminal Police Organization, 2021.

JERMAN BLAŽIČ, Borka; KLOBUČAR, Tomaž. Removing the barriers in cross-border crime investigation by gathering electronic evidence in an interconnected society. **Information & Communications Technology Law,** London, v. 29, n. 1, p. 66-81, 2020. DOI: 10.1080/13600834.2020.1705035.

NAÇÕES UNIDAS. **Convenção das Nações Unidas contra o Crime Cibernético.** Nova York: Organização das Nações Unidas, 2024.

RUOHONEN, Jukka. Recent trends in cross-border data access by law enforcement agencies. **arXiv,** Ithaca, 2023. DOI: 10.48550/arXiv.2302.09942.

SPIEZIA, Filippo. International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. **ERA Forum,** Heidelberg, v. 23, n. 1, p. 101-108, 2022. DOI: 10.1007/s12027-022-00707-8.

SVANTESSON, Dan Jerker B. **Solving the Internet jurisdiction puzzle.** Oxford: Oxford University Press, 2017.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Comprehensive study on cybercrime.** Vienna: United Nations, 2013.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **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.** Vienna: United Nations, 2024.

---

[1] Graduada em Direito pela Faculdade Jorge Amado - Salvador/Bahia - Brasil Pós-graduada em Direito Público pela JusPodivm - Salvador/Bahia -Brasil. E-mail: acesse o artigo original para visualizar o e-mail

[2] Graduado em Turismo pela Faculdade Unyahna (Salvador-BA) Pós-graduado em Direito Público pela Faculdade Legale em (São Paulo-SP). E-mail: acesse o artigo original para visualizar o e-mail

[3] Graduado em Administração de Empresas - Faculdade Ruy Barbosa - Salvador-BA, Brasil Pós-graduado em Direito Constitucional - Faculdade Integrada da Grande Fortaleza - Fortaleza-CE, Brasil. E-mail: acesse o artigo original para visualizar o e-mail

[4] Graduado em Direito - Faculdade Jorge Amado - Salvador, BA, Brasil Pós-graduado em Direito do Estado - Associação Educacional Unyahna - Salvador, BA, Brasil. E-mail: acesse o artigo original para visualizar o e-mail