CRIMES CIBERNÉTICOS: desafios à responsabilização penal na era digital.

Letícia Leite Machado

RESUMO

Os crimes cibernéticos representam um dos principais desafios contemporâneos ao sistema penal brasileiro, especialmente no que se refere à responsabilização de seus autores e à validade da prova digital. A volatilidade das evidências eletrônicas, as dificuldades de identificação individualizada em ambientes marcados pelo anonimato e a dimensão transnacional das infrações digitais dificultam significativamente a persecução penal. O presente artigo analisa os principais entraves à responsabilização penal por crimes cibernéticos no ordenamento jurídico brasileiro, com enfoque na prova digital, na preservação de sua integridade e nos mecanismos de cooperação internacional. A partir de pesquisa bibliográfica e análise jurisprudencial recente dos Tribunais Superiores, verifica-se que, embora o ordenamento jurídico tenha avançado com a edição de legislações específicas voltadas ao ambiente digital, ainda persistem lacunas relacionadas à tipificação de condutas emergentes, à padronização dos procedimentos periciais e à estrutura investigativa necessária à adequada produção probatória. Destaca-se, nesse contexto, o papel da função *hash* como instrumento técnico de verificação de integridade dos dados, sem afastar a necessidade de rigorosa documentação dos procedimentos de coleta, armazenamento e extração das evidências digitais. Conclui-se que a efetiva responsabilização penal em matéria cibernética depende não apenas de aperfeiçoamentos legislativos, mas também do fortalecimento institucional, da capacitação técnica dos agentes envolvidos e da ampliação dos mecanismos de cooperação internacional.

Palavras-chave: crimes cibernéticos; prova digital; função *hash*; cooperação internacional.

ABSTRACT

Cybercrime represents one of the main contemporary challenges to the Brazilian criminal justice system, particularly regarding the attribution of criminal liability and the validity of digital evidence. The volatility of electronic evidence, the difficulties in identifying individual conduct in anonymous environments, and the transnational nature of digital offenses significantly hinder criminal prosecution. This article examines the main obstacles to criminal liability for cybercrimes within the Brazilian legal system, focusing on digital evidence, the preservation of evidentiary integrity, and international cooperation mechanisms. Based on bibliographic research and recent case law analysis from the Superior Courts, the study demonstrates that, although the Brazilian legal framework has advanced through the enactment of legislation specifically directed at the digital environment, important gaps still remain concerning the typification of emerging conduct, the standardization of forensic procedures, and the investigative structure required for proper evidentiary production. In this context, the hash function is highlighted as a technical mechanism for verifying data integrity, without eliminating the need for rigorous documentation of procedures involving the collection, storage, and extraction of digital evidence. The study concludes that effective criminal accountability in cybercrime cases depends not only on legislative improvements, but also on institutional strengthening, technical training of public agents, and the expansion of international cooperation mechanisms.

Keywords: cybercrime; digital evidence; hash function.

1 INTRODUÇÃO

A intensa digitalização das relações sociais, econômicas e institucionais transformou profundamente a dinâmica da sociedade contemporânea. A expansão do uso da internet, das plataformas digitais e dos sistemas informáticos ampliou significativamente a circulação de informações e a conectividade global, mas também criou possibilidades para a prática de condutas ilícitas em ambiente virtual.

Nesse contexto, os crimes cibernéticos assumem crescente relevância jurídico-penal, especialmente em razão de características próprias do ciberespaço, como o anonimato, a velocidade de disseminação de dados, a volatilidade das informações e a ausência de barreiras territoriais.

Os delitos informáticos não se restringem à mera adaptação de crimes tradicionais ao meio digital. Muitas dessas condutas, como invasões de dispositivos, ataques de ransomware, fraudes eletrônicas e violações a infraestruturas críticas, somente se tornam possíveis em razão da própria estrutura tecnológica que sustenta o ambiente virtual, exigindo respostas normativas e investigativas específicas (PECK, 2023, p. 18).

Em razão disso, o Direito Penal e o Processo Penal passaram a enfrentar novos desafios relacionados à identificação de autoria, à obtenção de provas válidas e à preservação das garantias fundamentais no contexto digital.

No Brasil, houve importantes avanços legislativos voltados à disciplina do ambiente cibernético, com destaque para a Lei nº 12.737/2012 (Lei Carolina Dieckmann), o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a Lei01nº 13.964/2019 (Pacote Anticrime), além da Lei nº 14.155/2021 (BRASIL, 2012, 2014, 2018a, 2019a, 2021a).

Apesar disso, a efetiva responsabilização penal por ilícitos digitais ainda encontra obstáculos relevantes, sobretudo diante da sofisticação tecnológica empregada pelos agentes e da dificuldade de adaptação das estruturas investigativas tradicionais à realidade digital.

A atribuição individualizada da autoria, por exemplo, frequentemente é dificultada pela utilização de redes privadas virtuais (VPN), servidores proxy, protocolos de anonimização e compartilhamento de endereços IP, circunstâncias que exigem dados técnicos complementares para a identificação do usuário responsável. Paralelamente, a prova digital apresenta elevada fragilidade quanto à sua preservação, tendo em vista a facilidade de alteração, supressão ou manipulação do conteúdo eletrônico.

Nesse cenário, tornam-se indispensáveis mecanismos rigorosos de preservação da integridade probatória, especialmente no que se refere à rastreabilidade dos vestígios digitais e à observância de protocolos técnicos de documentação, armazenamento e extração de dados, nos quais a função hash desempenha relevante papel de verificação de integridade. Soma-se a isso a dimensão transnacional dos delitos cibernéticos, que demanda instrumentos céleres e eficientes de cooperação internacional, ainda insuficientemente estruturados na prática investigativa nacional (FERNANDES; GUIMARÃES, 2025, p. 6).

Ante o exposto, o presente trabalho tem como objetivo geral analisar os principais desafios relacionados à responsabilização penal por crimes cibernéticos no ordenamento jurídico brasileiro, com enfoque nas dificuldades probatórias, na validade da prova digital, na atribuição de autoria e nos mecanismos de cooperação internacional.

Como objetivos específicos, pretende-se: (i) examinar o marco normativo aplicável aos crimes cibernéticos no Brasil; (ii) analisar os desafios relacionados à produção e preservação da prova digital; (iii) discutir a relevância da função hash como mecanismo técnico de garantia de integridade dos dados; (iv) investigar os entraves relacionados à identificação dos autores em ambientes digitais anônimos; e (v) avaliar os avanços e limitações da cooperação internacional no combate à criminalidade cibernética.

A pesquisa adota metodologia bibliográfica e jurisprudencial, baseada na análise de doutrina especializada, legislação pertinente e precedentes recentes dos Tribunais Superiores. Parte-se da hipótese de que, embora o ordenamento jurídico brasileiro tenha evoluído significativamente na regulamentação do ambiente digital, ainda persiste um descompasso entre a crescente sofisticação dos crimes cibernéticos e a capacidade estatal de investigar, preservar provas válidas e promover a responsabilização penal de maneira efetiva, sem afastamento das garantias fundamentais do devido processo legal.

2 CRIMES CIBERNÉTICOS: CONCEITOS E MARCO NORMATIVO

2.1 DELIMITAÇÕES CONCEITUAIS

Os crimes virtuais, também denominados crimes cibernéticos ou delitos informáticos, consistem em infrações penais praticadas por meio da internet, de dispositivos eletrônicos ou de sistemas computacionais, bem como aquelas que têm tais estruturas tecnológicas como alvo direto. Essas condutas ilícitas utilizam o ambiente digital para atingir bens jurídicos tutelados

pelo Direito, como patrimônio, honra, intimidade, privacidade, segurança da informação e liberdade individual. A utilização do ciberespaço proporciona aos infratores elevado alcance de propagação, rapidez na execução das condutas e significativo grau de anonimato, além de permitir que os efeitos do delito ultrapassem fronteiras territoriais em poucos segundos.

A crescente dependência social, econômica e institucional das tecnologias digitais contribuiu para a ampliação da incidência desse tipo de criminalidade, tornando os sistemas informáticos ambientes particularmente vulneráveis à atuação ilícita. Nesse cenário, ataques virtuais passaram a atingir não apenas indivíduos, mas também empresas privadas, instituições financeiras e órgãos públicos, ocasionando prejuízos patrimoniais, violação de dados pessoais e comprometimento de serviços essenciais.

Segundo Greco (2020, p. 602), os crimes cibernéticos podem ser classificados, predominantemente, em duas categorias: crimes próprios (ou puros) e crimes impróprios, de acordo com o grau de dependência tecnológica necessário à prática da conduta. Os crimes próprios são aqueles cuja existência depende necessariamente do ambiente digital, uma vez que têm como objeto direto sistemas informáticos, dispositivos eletrônicos ou dados digitais. Inserem-se nessa categoria delitos como invasão de dispositivo informático, disseminação de malware, ataques de ransomware, interceptação indevida de dados e clonagem de identidade digital.

Por outro lado, os crimes impróprios correspondem a infrações penais tradicionais que passaram a ser executadas por meio de ferramentas tecnológicas e plataformas digitais. Nesses casos, o ambiente virtual funciona como instrumento de facilitação da prática criminosa, sem alterar substancialmente a essência da conduta típica. Exemplificativamente, enquadram-se nessa categoria delitos como estelionato eletrônico, ameaças, calúnia, difamação, perseguição virtual e fraudes bancárias praticadas por aplicativos ou redes sociais.

Embora essa classificação possua caráter predominantemente doutrinário e analítico, sua utilização revela-se relevante para a compreensão das diferentes formas de manifestação da criminalidade digital.

Essa distinção evidencia que nem toda prática ilícita ocorrida na internet demanda a criação de novo tipo penal, podendo muitas condutas ser adequadamente enquadradas em figuras típicas já existentes no ordenamento jurídico, desde que respeitados os limites impostos pelo princípio da legalidade estrita.

Ao mesmo tempo, a categorização demonstra que determinadas condutas direcionadas especificamente contra sistemas informáticos, bancos de dados e estruturas tecnológicas

exigem tipificação própria, diante da especificidade dos bens jurídicos atingidos e da insuficiência das figuras penais tradicionais para abarcar integralmente tais comportamentos. Nesse sentido, a ausência de previsão normativa adequada pode gerar lacunas de tutela penal em relação a bens de elevada relevância na sociedade digital contemporânea, especialmente diante da crescente sofisticação técnica dos ataques cibernéticos (BITENCOURT, 2026, p. 569).

2.2 LEGISLAÇÃO APLICÁVEL

O ordenamento jurídico brasileiro respondeu de forma gradual ao fenômeno dos crimes cibernéticos. Durante certo período, buscou-se enquadrar condutas novas em tipos tradicionais, como o estelionato, previsto no art. 171 do Código Penal Brasileiro (BRASIL 1940).

Todavia, tal adequação gerou diversos debates acerca da suposta insuficiência dessas figuras para lidar com ataques sofisticados a sistemas informáticos. Assim, a evolução legislativa ocorreu de forma fragmentada e, em muitos casos, diante da necessidade de reprimir crimes midiáticos de grande repercussão (GRECO, 2020, p. 603).

A promulgação da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, representou um importante marco legislativo no enfrentamento dos crimes praticados em ambiente digital no Brasil. A norma introduziu no Código Penal o art. 154-A, responsável por tipificar a invasão de dispositivo informático alheio com o objetivo de obter, adulterar ou destruir dados e informações, bem como instalar vulnerabilidades destinadas à obtenção de vantagem ilícita. A criação desse tipo penal demonstrou a necessidade de adaptação do ordenamento jurídico às novas formas de criminalidade decorrentes da expansão tecnológica e do uso massivo da internet (BRASIL, 2012).

Posteriormente, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) contribuíram para o fortalecimento do arcabouço normativo relacionado ao ambiente digital. Embora não possuam enfoque penal direto, tais diplomas estabeleceram importantes diretrizes acerca da proteção de dados, responsabilidade dos provedores, preservação de registros eletrônicos e tutela da privacidade no meio virtual, aspectos frequentemente relacionados às investigações de delitos cibernéticos (BRASIL, 2014, 2018a).

No ano de 2019, a Lei nº 13.964/2019, denominada Pacote Anticrime, introduziu os arts. 158-A a 158-F no Código de Processo Penal, regulamentando formalmente a cadeia de

custódia no ordenamento jurídico brasileiro. Apesar de os dispositivos não fazerem referência expressa às evidências digitais, seus parâmetros passaram a ser amplamente aplicados à prova eletrônica, exigindo rastreabilidade, preservação da integridade e documentação detalhada dos procedimentos adotados desde a coleta até a apresentação do material em juízo. Tal inovação revelou-se especialmente relevante diante da elevada suscetibilidade de manipulação das evidências digitais e da necessidade de assegurar confiabilidade à atividade probatória (BRASIL, 2019a).

Ademais, a Lei nº 14.155/2021 promoveu alterações no Código Penal para agravar as penas dos crimes de furto e estelionato praticados por meio eletrônico ou mediante fraude digital. A reforma legislativa evidenciou o reconhecimento, pelo legislador, do expressivo impacto social, econômico e patrimonial provocado pelos golpes virtuais, cuja incidência se intensificou com a ampliação das relações digitais e dos meios eletrônicos de pagamento (BRASIL, 2021a).

A despeito desses avanços, subsiste a discussão acerca da insuficiência do atual catálogo de tipos penais para abranger condutas emergentes, como ataques de ransomware em larga escala, a comercialização de serviços voltados à prática de ataques cibernéticos (crime-as-a-service) e a exploração de vulnerabilidades em cadeias de suprimento de software (SILVA; FAYÃO, 2025, p. 158).

A necessidade de enfrentamento da criminalidade cibernética e de efetiva tutela dos bens jurídicos no ambiente digital não pode servir de fundamento para a ampliação indiscriminada do ius puniendi por meio de construções interpretativas excessivamente expansivas. Isso porque a atuação estatal em matéria penal encontra limites no princípio da legalidade, o qual exige tipificação prévia e estrita das condutas incriminadas, impedindo a criação ou ampliação de tipos penais por analogia ou interpretação extensiva em prejuízo do acusado (ALENCAR, 2024, p. 164).

3 PROVA DIGITAL, CADEIA DE CUSTÓDIA E FUNÇÃO *HASH*

3.1 PROVA DIGITAL E SUAS PECULIARIDADES

A prova digital pode ser entendida como toda informação de interesse para o processo penal armazenada ou transmitida em formato eletrônico, seja em dispositivos físicos (computadores, smartphones, discos rígidos, mídias removíveis), seja em ambientes de

computação em nuvem ou em trânsito por redes de comunicação. Diferentemente de objetos materiais, os dados digitais são extremamente voláteis, podendo ser copiados ou apagados com facilidade, alterados sem deixar marcas visíveis a olho nu e armazenados em locais fisicamente distantes da jurisdição que conduz a investigação (FERNANDES; GUIMARÂES, 2025, p. 9).

Essas características geram, ao menos, três desafios centrais, quais sejam: garantir a integridade da informação, isto é, que o dado analisado pelo perito ou apresentado em juízo seja o mesmo que foi coletado na fonte; assegurar a autenticidade e a origem do dado, permitindo vincular o conteúdo a determinado dispositivo, conta ou usuário; e preservar a rastreabilidade de todas as intervenções realizadas sobre a prova, para possibilitar o controle pelas partes e pelo juiz (SILVA; FAYÃO, 2025, p. 158).

A resposta normativa brasileira a esses desafios se encontra, em boa medida, na disciplina da cadeia de custódia da prova, introduzida no Código de Processo Penal pela Lei 13.964/2019, e em orientações técnicas produzidas por órgãos de persecução penal e por peritos oficiais (BRASIL, 2019a).

3.2 CADEIA DE CUSTÓDIA DA PROVA DIGITAL

A cadeia de custódia, nos termos do art. 158-A do Código de Processo Penal, compreende o conjunto de procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, de modo a rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte (ALENCAR, 2024, p. 858). Transposta para o universo digital, essa sistematica exige que, desde o primeiro contato com um dispositivo ou dado eletrônico potencialmente relevante, todas as etapas sejam registradas adequadamente.

Isso demanda a adoção de diversas medidas voltadas à preservação da rastreabilidade e integridade da prova digital, tais como o registro da autoridade responsável pela apreensão do dispositivo eletrônico, das circunstâncias da coleta e das ferramentas utilizadas, bem como da data e horário do procedimento. Também se faz necessária a documentação detalhada da extração dos dados, com indicação da utilização de cópias forenses, dos softwares empregados e da eventual necessidade de superação de mecanismos de senha ou criptografia. Soma-se a isso a geração de valores hash para verificação da integridade dos arquivos e o controle contínuo de acesso às mídias e aos relatórios periciais, a fim de evitar manipulações indevidas do material probatório (FERNANDES; GUIMARÃES, 2025, p. 12).

A ausência ou insuficiência dessa documentação pode comprometer a confiabilidade da prova digital e suscitar questionamentos acerca de sua autenticidade e integridade, especialmente em hipóteses envolvendo comunicações privadas, dados de geolocalização ou conteúdos armazenados em nuvem.

3.3 A FUNÇÃO *HASH* COMO GARANTIA DE INTEGRIDADE

Nesse cenário, a função *hash* assume papel de destaque como ferramenta técnica de reforço à cadeia de custódia da prova digital. Em termos simplificados, funções *hash* criptográficas são algoritmos que recebem um conjunto de dados como entrada (por exemplo, um arquivo, uma pasta ou uma imagem forense de disco) e produzem uma sequência fixa de caracteres (o valor *hash*), de modo que qualquer alteração, mesmo mínima, no conjunto de dados de origem gera um resultado completamente distinto (FISBERG, 2025, p. 5).

Do ponto de vista probatório, o uso de *hashes* permite que se ateste, com elevado grau de segurança, que um arquivo analisado em momento posterior é idêntico ao arquivo originalmente coletado. Basta que, no ato da apreensão ou da extração forense, seja gerado e registrado o valor hash do conteúdo; em etapas subsequentes, pode-se recalcular o *hash* do mesmo material e compará-lo com o valor inicial. Se coincidirem, há forte indicativo de que o dado permaneceu íntegro ao longo da cadeia de custódia (BADARÓ, 2021, p. 8).

Assim, é importante destacar que o uso de tal função não substitui a cadeia de custódia, mas a complementa. A integridade matemática assegurada pelo *hash* precisa ser inserida em um contexto procedimental mais amplo, que documente quem teve acesso ao material, em que condições e com quais finalidades, de forma que tal função reforça a confiabilidade do vestígio digital, mas não resolve, por si só, eventuais problemas relacionados à licitude da coleta (como buscas ilegais) ou à violação de direitos fundamentais (como o sigilo das comunicações).

Além disso, deve-se reconhecer os limites dessa aplicação. A escolha de algoritmos obsoletos ou vulneráveis, bem como a ausência de padronização sobre qual função utilizar e em que momento aplicá-la, pode comprometer a força probatória do recurso. Por essa razão, órgãos de perícia e investigações costumam adotar algoritmos amplamente reconhecidos pela comunidade técnica e registrar, nos laudos, não apenas o valor *hash*, mas também o algoritmo empregado, a data e hora da geração e o contexto da operação (BADARÓ, 2021, p. 9).

3.4 A JURISPRUDÊNCIA SOBRE PROVA DIGITAL E NULIDADES

O Superior Tribunal de Justiça (STJ) tem enfrentado, com crescente frequência, controvérsias relacionadas à validade da prova digital e à observância da cadeia de custódia. Embora a matéria ainda não conte com jurisprudência integralmente consolidada, já é possível identificar diretrizes interpretativas progressivamente adotadas pela Corte.

Em maio de 2024, a Quinta Turma do STJ, ao julgar o AgRg no HC 828.054/RN, reconheceu a inadmissibilidade de provas obtidas por meio de capturas de tela de conversas de WhatsApp extraídas de aparelho celular sem observância de metodologia técnica adequada. Na ocasião, o relator, Ministro Joel Ilan Paciornik, ressaltou que as provas digitais são facilmente passíveis de alteração, inclusive de forma imperceptível, razão pela qual exigem rigor reforçado quanto à preservação da cadeia de custódia (BRASIL, 2024a).

Ainda em 2024, no julgamento do RHC 205.441/GO, o Ministro Rogério Schietti Cruz declarou a nulidade de provas extraídas de aparelho celular apreendido durante operação conduzida pelo Ministério Público de Goiás. O dispositivo não possuía lacre, tampouco havia registro do respectivo IMEI, circunstâncias que levaram-no a concluir que o Estado não demonstrou adequadamente a higidez das informações digitais obtidas (BRASIL, 2024b).

No ano seguinte, em em 2025, no HC 943.895/PR, a Quinta Turma determinou o desentranhamento de provas digitais em razão de a autoridade policial ter acessado previamente o conteúdo do aparelho celular antes da realização da perícia técnica, o que, segundo o relator Ministro Joel Ilan Paciornik, comprometeu a integridade da evidência digital (BRASIL, 2025a).

Observa-se que o entendimento do STJ converge no sentido da exigência mínima de documentação acerca dos procedimentos de coleta, armazenamento e análise da prova digital, afastando a simples apresentação do arquivo desacompanhada de informações sobre sua origem, preservação e cadeia de custódia. Tal posicionamento foi consolidado no Informativo nº 763, segundo o qual "são inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos" (BRASIL, 2023a).

O entendimento predominante no Superior Tribunal de Justiça é no sentido de que a quebra da cadeia de custódia não acarreta, por si só, a nulidade automática da prova. Nesse contexto, a Sexta Turma, ao julgar o HC 653.515/RJ, firmou orientação de que eventuais

irregularidades devem ser analisadas pelo magistrado em conjunto com os demais elementos produzidos na instrução criminal, a fim de verificar se a prova impugnada ainda preserva grau suficiente de confiabilidade (BRASIL, 2021b).

Dessa forma, incide o disposto no art. 563 do Código de Processo Penal quando inexistente demonstração concreta de prejuízo à credibilidade do material probatório. Tal posicionamento reflete a aplicação do princípio do pas de nullité sans grief, segundo o qual não há nulidade sem demonstração de prejuízo, evidenciando uma tendência jurisprudencial de análise casuística da cadeia de custódia, em consonância com as particularidades fáticas de cada caso concreto (BRASIL, 1941).

Assim, eventuais irregularidades devem ser ponderadas à luz da confiabilidade efetiva da prova e do conjunto probatório produzido, afastando-se a decretação automática de nulidade. Nessa linha, o STJ já decidiu que "não se acolhe alegação de quebra na cadeia de custódia quando vier desprovida de qualquer outro elemento que indique adulteração [...]" (BRASIL, 2021c).

Todavia, nas hipóteses em que a irregularidade compromete o exercício efetivo do contraditório e da ampla defesa o Superior Tribunal de Justiça tem reconhecido a nulidade da prova produzida. Nesse sentido, no julgamento do RHC 218.358/PI, em novembro de 2025, a Corte declarou a nulidade dos laudos periciais em razão da impossibilidade de a defesa ter acesso às mídias originais utilizadas na perícia, circunstância que inviabilizou a verificação da autenticidade e integridade do material probatório (BRASIL, 2025b).

Em contrapartida, o devido processo legal probatório impede a atribuição de valor determinante a conteúdos digitais cuja integridade não possa ser tecnicamente comprovada, uma vez que, no âmbito das evidências digitais, a dúvida acerca da autenticidade do material não constitui mera hipótese abstrata, mas risco inerente ao próprio meio tecnológico.

Com isso, preserva-se o núcleo do entendimento firmado pela Sexta Turma no REsp 2.123.764/ES, segundo o qual determinados conteúdos digitais, uma vez formalizados e regularmente juntados aos autos, podem ser valorados sob a lógica da prova documental, sem exigência automática de perícia técnica complexa. Todavia, tal compreensão não afasta a necessidade de controle rigoroso de confiabilidade quando houver impugnação substancial acerca da autenticidade ou integridade do material apresentado (BRASIL, 2024c).

Nesse contexto, mantém-se a compatibilidade com a orientação adotada pela Quinta Turma no AREsp 2.972.295/MT, que reforça a imprescindibilidade de observância de critérios técnicos de verificação quando a prova digital assume papel determinante para a formação do

convencimento judicial. Em matéria de prova digital, a confiabilidade não decorre da autoridade de quem acessou ou produziu o conteúdo, mas da possibilidade de reexecução, rastreabilidade e controle técnico por terceiros independentes, mediante registro verificável dos procedimentos empregados, incluindo a identificação da ferramenta utilizada, da mídia examinada, do momento da coleta e das garantias de preservação da integridade do resultado obtido (BRASIL, 2025c).

Essa via conciliatória revela-se a mais adequada à preservação do devido processo legal probatório em um cenário marcado pela crescente sofisticação dos mecanismos de manipulação, adulteração e reconstrução artificial da realidade informacional.

É nesse cenário que a função hash merece destaque, notadamente na preservação da cadeia de custódia da prova digital no processo penal. A jurisprudência recente do STJ tem reconhecido a relevância de mecanismos técnicos aptos a garantir a integridade e autenticidade das evidências digitais.

No Inq 1674/DF, julgado pela Corte Especial em 2026, destacou-se que a perícia realizou cópia por espelhamento mediante utilização da função hash, capaz de comprovar que os dados extraídos eram idênticos aos constantes do dispositivo apreendido. De igual modo, no AREsp 2.972.295/MT, a Quinta Turma reconheceu que a utilização da ferramenta Cellebrite associada ao algoritmo hash preservou a cadeia de custódia e assegurou a confiabilidade da prova digital (BRASIL, 2026, 2025c).

Assim, observa-se a consolidação do entendimento de que a função hash constitui importante mecanismo técnico de verificação da integridade das evidências digitais no processo penal.

O Supremo Tribunal Federal (STF), por sua vez, adota uma postura de rigorosa proteção aos direitos fundamentais na internet, consolidando que o combate aos cibercrimes não pode se sobrepor às garantias constitucionais da intimidade, da privacidade e do devido processo legal. A corte rejeita ordens judiciais genéricas de quebra de sigilo tecnológico, como no RE 1301250/Tema 1148, que discute a legalidade de ordens abrangentes de varredura de dados de busca no Google), exigindo nexo de causalidade estrito e especificidade para afastar o chamado fishing expedition (pesca probatória especulativa) (BRASIL, 2021d).

Adicionalmente, o tribunal atua firmemente contra a nulidade de provas colhidas sem o cumprimento das formalidades legais: no AReg na AP 1030/DF, reafirmou-se a indispensabilidade de autorização judicial prévia para o acesso a dados de aparelhos celulares ou contas digitais. Paralelamente, em decisões históricas sobre o ecossistema digital, como no

julgamento da ADIs 5527 e do RE 1037396, o STF expandiu os deveres de vigilância das redes sociais em crimes graves, exigindo a derrubada imediata de conteúdos ilícitos e crimes virtuais após notificação extrajudicial, demonstrando um equilíbrio entre a repressão penal na internet e o respeito irrestrito à barreira dos direitos individuais (BRASIL, 2018b, 2023b, 2025d).

4 DESAFIOS CENTRAIS À RESPONSABILIZAÇÃO PENAL

4.1 DIFICULDADES DE IDENTIFICAÇÃO E ATRIBUIÇÃO DE AUTORIA

A atribuição de condutas ilícitas em ambiente digital a indivíduos determinados constitui, talvez, o maior obstáculo à responsabilização penal. Enquanto no mundo físico a autoria pode ser estabelecida por testemunhas, vestígios biológicos ou imagens de câmeras de segurança, no ciberespaço o "rastro digital" é frequentemente mascarado, o que dificulta a aplicação das normas tradicionais do direito penal (BORGES, 2024).

Técnicas como o uso de redes privadas virtuais (VPN), servidores proxy, protocolos TOR e criptografia de extremo a extremo permitem que o agente atue de forma praticamente anônima, dificultando a vinculação da conduta a uma pessoa física (BITENCOURT, 2026, p. 261). Além disso, a possibilidade de compartilhamento de um mesmo endereço IP por múltiplos usuários, especialmente em redes residenciais ou corporativas, amplia as dificuldades relacionadas à identificação precisa do verdadeiro autor da conduta ilícita.

No julgamento dos REsp 1.777.769/SP e REsp 2.170.872/SP, o STJ pacificou que o fornecimento do IP de forma isolada é inútil e insuficiente para individualizar o autor. Isoo porque como faltam números de IP no padrão IPv4, os provedores distribuem o mesmo IP público para dezenas ou centenas de usuários simultaneamente (BRASIL, 2019b, 2025e).

Logo, para garantir a individualização do internauta, o STJ tem exigido que, além do IP, os provedores forneçam a porta lógica, dado técnico que identifica exatamente qual aparelho ou aplicação realizou a conexão na hora do fato. Sem a porta lógica, é impossível saber qual dos múltiplos usuários conectados àquele IP cometeu a infração.

4.2 COMPETÊNCIA JURISDICIONAL E TRANSNACIONALIDADE

A natureza transnacional dos crimes cibernéticos impõe a cooperação internacional como requisito indispensável para a efetividade da persecução penal. Diferentemente dos

delitos tradicionais, as infrações praticadas em ambiente digital frequentemente ultrapassam fronteiras territoriais em questão de segundos, envolvendo agentes, servidores, vítimas e provedores localizados em diferentes países. Em razão disso, a atuação isolada de um único Estado revela-se insuficiente para identificar autores, preservar provas digitais e responsabilizar os envolvidos, sobretudo diante da velocidade de propagação dos ataques e da facilidade de ocultação da identidade dos agentes.

Nesse cenário, a cooperação jurídica internacional assume papel central no combate à criminalidade cibernética, permitindo o intercâmbio de informações, a preservação de dados eletrônicos e a realização coordenada de investigações transnacionais. A necessidade de respostas mais céleres decorre, especialmente, da volatilidade das evidências digitais, que podem ser rapidamente alteradas, apagadas ou transferidas entre servidores localizados em diferentes jurisdições. Assim, a demora nos mecanismos tradicionais de cooperação, como cartas rogatórias e pedidos diplomáticos convencionais, mostra-se incompatível com a dinâmica dos crimes informáticos contemporâneos.

Nesse contexto, a Convenção de Budapeste sobre o Cibercrime, adotada em 2001 pelo Conselho da Europa, consolidou-se como o principal instrumento internacional voltado ao enfrentamento dos delitos cibernéticos. O tratado foi pioneiro ao estabelecer parâmetros mínimos de tipificação penal e mecanismos específicos de cooperação jurídica voltados à realidade digital, buscando harmonizar a atuação dos Estados signatários diante da crescente complexidade da criminalidade virtual (CONSELHO DA EUROPA, 2001).

Dentre os instrumentos previstos pela Convenção destacam-se a preservação expedita de dados armazenados, a coleta em tempo real de dados de tráfego e a criação de canais permanentes de comunicação entre autoridades centrais.

A adesão do Brasil à Convenção de Budapeste, formalizada pelo Decreto nº 11.131/2023, representa importante avanço estratégico no fortalecimento da capacidade investigativa nacional em matéria cibernética. A incorporação do tratado ao ordenamento jurídico brasileiro ampliou as possibilidades de cooperação direta com autoridades estrangeiras e reduziu entraves burocráticos tradicionalmente presentes nos pedidos internacionais de obtenção de provas digitais. Além disso, o sistema de funcionamento ininterrupto entre autoridades centrais, disponível vinte e quatro horas por dia, mostra-se especialmente relevante diante da necessidade de respostas imediatas para preservação de dados eletrônicos (MINISTÉRIO DA JUSTIÇA, 2023).

A importância desse modelo cooperativo torna-se ainda mais evidente diante da crescente profissionalização da criminalidade cibernética. Atualmente, organizações criminosas especializadas operam de maneira estruturada e descentralizada, oferecendo serviços ilícitos em plataformas clandestinas, como comercialização de malware, ataques de ransomware, invasão de sistemas e vazamento de dados pessoais. Muitas dessas atividades são desenvolvidas a partir de países com baixa capacidade regulatória ou reduzida cooperação internacional, circunstância que dificulta significativamente a responsabilização penal dos agentes envolvidos.

Paralelamente, o Brasil também participa da construção de um novo marco internacional sob a coordenação da Organização das Nações Unidas. Em 2024, foi aprovado o texto da Convenção da ONU sobre Crimes Cibernéticos, instrumento que busca ampliar a cooperação global e incentivar a criação de estruturas normativas mínimas em países que ainda não dispõem de legislação específica sobre o tema. O Brasil exerceu posição de destaque nas negociações, atuando como vice-presidente dos debates diplomáticos relacionados ao tratado (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2024).

O novo tratado da ONU busca enfrentar um dos principais problemas relacionados ao combate transnacional ao cibercrime: a existência de “brechas geográficas”, caracterizadas por jurisdições que não possuem mecanismos adequados de repressão ou cooperação investigativa. Nessas localidades, a ausência de legislação específica, estrutura técnica ou integração internacional favorece a atuação de grupos criminosos que exploram tais fragilidades institucionais para dificultar investigações e evitar responsabilização.

Não obstante os avanços normativos, a efetividade da cooperação internacional depende da existência de estruturas operacionais especializadas e de constante atualização tecnológica. Nesse aspecto, diversos países já desenvolveram órgãos específicos voltados ao enfrentamento da criminalidade digital. A União Europeia, por exemplo, conta com o European Cybercrime Centre (EC3), vinculado à Europol, enquanto os Estados Unidos possuem a Cyber Division do FBI, responsável pela coordenação de investigações relacionadas a delitos cibernéticos em âmbito federal.

No Brasil, observa-se progressivo fortalecimento institucional da Polícia Federal no combate aos crimes informáticos, especialmente por meio da ampliação das atividades da Divisão de Repressão a Crimes Cibernéticos. Nesse contexto, destaca-se o acordo de cooperação firmado entre a Polícia Federal e a Europol em 2025, voltado ao compartilhamento

de inteligência, intercâmbio de informações e realização de investigações conjuntas relacionadas à criminalidade transnacional (EUROPOL, 2025).

Um dos exemplos mais emblemáticos da relevância da cooperação internacional no combate ao cibercrime foi a Operação Emotet, deflagrada em 2021. A ação resultou na desarticulação de uma das maiores estruturas de malware bancário do mundo, responsável por ataques que atingiram instituições financeiras, empresas privadas e órgãos públicos em diversos países. Coordenada pela Europol, a operação envolveu a atuação conjunta de autoridades policiais de mais de dez nações, além da colaboração direta de empresas de tecnologia e segurança digital. O êxito da operação decorreu justamente da rapidez no compartilhamento de informações e da integração técnica entre os participantes (SILVA; FAYÃO, 2025, p. 171).

O caso evidencia que o enfrentamento efetivo da criminalidade cibernética depende de uma atuação articulada entre Estados, organismos internacionais e setor privado, especialmente diante da natureza descentralizada e altamente sofisticada das ameaças digitais contemporâneas. Nesse sentido, a cooperação internacional deixa de representar mera ferramenta auxiliar e passa a constituir elemento estrutural indispensável à efetiva responsabilização penal no ciberespaço.

5 CONSIDERAÇÕES FINAIS

A análise das seções e subseções precedentes confirma que a responsabilização penal por crimes cibernéticos no Brasil enfrenta desafios estruturais que vão além da mera tipificação de condutas. Conquanto o ordenamento jurídico tenha evoluído significativamente nos últimos anos, com a introdução de tipos penais específicos, a regulação do ambiente digital pelo Marco Civil da Internet e a adesão à Convenção de Budapeste, persiste uma lacuna crítica entre o texto legal e sua aplicação prática, especialmente no que diz respeito à prova e à cooperação internacional.

A prova digital, por sua volatilidade e susceptibilidade à adulteração, exige procedimentos rigorosos de cadeia de custódia, conforme destacado tanto pela doutrina quanto pela jurisprudência do STJ. A função hash surge como ferramenta técnica valiosa para atestar a integridade dos dados, mas, como bem ressaltado, não substitui a necessidade de documentação completa do percurso da prova, desde a apreensão até a análise pericial. A jurisprudência já caminha em direção a um equilíbrio: rejeita a nulidade automática por falhas

formais, mas exige demonstração concreta de prejuízo à defesa quando há rompimento na cadeia de custódia que inviabilize o contraditório.

Por outro lado, a atribuição de autoria permanece frágil. O uso de tecnologias de anonimização e a ausência de dados técnicos complementares, como a porta lógica, tornam a individualização do infrator uma tarefa complexa, muitas vezes impossível. Nesse ponto, a jurisprudência do STJ tem sido clara: o mero endereço IP, isoladamente, é insuficiente para sustentar uma condenação.

Finalmente, a cooperação internacional, embora reforçada pela adesão à Convenção de Budapeste e pela participação ativa nas negociações da nova Convenção da ONU, ainda enfrenta entraves burocráticos e operacionais. A efetividade dessa colaboração depende não apenas de tratados, mas de estruturas institucionais dedicadas e de acordos práticos com provedores globais.

Diante disso, conclui-se que o enfrentamento eficaz aos crimes cibernéticos exige uma abordagem multifacetada: aperfeiçoamento normativo pontual, mas, sobretudo, investimento em capacitação pericial, padronização de protocolos de investigação digital e fortalecimento dos canais de cooperação internacional. Somente assim será possível superar a sensação de impunidade que ainda cerca o ciberespaço, garantindo-se ao mesmo tempo a eficiência da persecução penal e o respeito aos direitos e garantias fundamentais.

REFERÊNCIAS

ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal*. 3. ed. São Paulo: Noeses, 2024.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção da prova na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, v. 29, n. 343, p. 7-9, jun. 2021. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 18 maio 2026.

BITENCOURT, Cezar R. *Tratado de Direito Penal: Parte Especial*, vol. 2. 26. ed. Rio de Janeiro: SRV, 2026. E-book. p. 569. ISBN 9786551771651. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786551771651/. Acesso em: 13 maio 2026.

BORGES, Beatriz. Crimes cibernéticos: como a legislação penal está se adaptando à nova realidade digital. *Blog do Direito IDP*, 25 nov. 2024. Disponível em: https://blog.idp.edu.br/juridico-avancado/crimes-ciberneticos-como-a-legislacao-penal-esta-se-adaptando-a-nova-realidade-digital/. Acesso em: 12 maio 2026.

BRASIL. Decreto-Lei n. 2.848, de 7 de dezembro de 1940. *Código Penal*. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 20 maio 2026.

BRASIL. Decreto-Lei n. 3.689, de 3 de outubro de 1941. *Código de Processo Penal*. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 20 maio 2026.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 — Código Penal; e dá outras providências. *Diário Oficial da União*, Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 maio 2026.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 maio 2026.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*, Brasília, DF, ano 155, n. 157, p. 59-64, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 maio 2026.

BRASIL. Lei n. 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. *Diário Oficial da União*, Brasília, DF, 24 dez. 2019a. Seção 1, edição extra, p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 15 maio 2026.

BRASIL. Lei n. 14.155, de 27 de maio de 2021. Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei n. 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. *Diário Oficial da União*, Brasília, DF, 28 maio 2021a. Seção 1, p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 15 maio 2026.

BRASIL. Decreto n. 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. *Diário Oficial da União*, Brasília, DF, 13 abr. 2023. Seção 1, p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491. Acesso em: 20 maio 2026.

BRASIL. Ministério da Justiça e Segurança Pública. *Convenção de Budapeste é promulgada no Brasil*. Brasília, DF, 17 abr. 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 20 maio 2026.

BRASIL. Superior Tribunal de Justiça. *Informativo de Jurisprudência* n. 763. Brasília, DF: STJ, 14 fev. 2023a. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?b=INFJ&materia=&orgao=&ano=&relator=&operador=e&thesaurus=JURIDICO&p=true&l=25&refinar=S+INPATH%28DISP%29&acao=pesquisar&dtdj=&dtde=&ordem=&isPesquisaDefault=false&pesquisaPorNumero=S&livre=763. Acesso em: 20 maio 2026.

BRASIL. Superior Tribunal de Justiça (3ª Turma). Recurso Especial n. 1.777.769/SP. Relatora: Min. Nancy Andrighi. Julgado em 05 nov. 2019b. *Diário da Justiça Eletrônico*, Brasília, 08 nov. 2019.

BRASIL. Superior Tribunal de Justiça (3ª Turma). Recurso Especial n. 2.170.872/SP. Relatora: Min. Nancy Andrighi. Julgado em 18 mar. 2025e. *Diário da Justiça Eletrônico*, Brasília, 21 mar. 2025.

BRASIL. Superior Tribunal de Justiça (5ª Turma). Agravo Regimental no Habeas Corpus n. 828.054/RN. Relator: Min. Joel Ilan Paciornik. Julgado em 23 abr. 2024a. *Diário da Justiça Eletrônico*, Brasília, 29 abr. 2024.

BRASIL. Superior Tribunal de Justiça (5ª Turma). Agravo Regimental no Habeas Corpus n. 943.895/PR. Relator: Min. Joel Ilan Paciornik. Julgado em 03 set. 2025a. *Diário da Justiça Eletrônico*, Brasília, 08 set. 2025.

BRASIL. Superior Tribunal de Justiça (5ª Turma). Agravo em Recurso Especial n. 2.972.295/MT. Relator: Min. Reynaldo Soares da Fonseca. Brasília, DF, julgado em 16 set2025c. *Diário da Justiça Eletrônico*, Brasília, 23 set. 2025.

BRASIL. Superior Tribunal de Justiça (5ª Turma). Habeas Corpus n. 653.515/RJ. Relator: Min. Rogerio Schietti Cruz. Julgado em 23 nov. 2021b. *Diário da Justiça Eletrônico*, Brasília, 01 fev. 2022.

BRASIL. Superior Tribunal de Justiça (6ª Turma). Agravo Regimental no Recurso em Habeas Corpus n. 125.733/SP. Relator: Min. Antonio Saldanha Palheiro. Julgado em 23 nov. 2021c. *Diário da Justiça Eletrônico*, Brasília, 26 nov. 2021.

BRASIL. Superior Tribunal de Justiça (6ª Turma). Habeas Corpus n. 831.357/RS. Relator: Min. Jesuíno Rissato. Julgado em 17 out. 2023. *Diário da Justiça Eletrônico*, Brasília, 20 out. 2023.

BRASIL. Superior Tribunal de Justiça (6ª Turma). Recurso Especial n. 2.123.764/ES. Relator: Min. Sebastião Reis Júnior. Julgado em 27 ago. 2024c. *Diário da Justiça Eletrônico*, Brasília, 02 set. 2024.

BRASIL. Superior Tribunal de Justiça (6ª Turma). Recurso Ordinário em Habeas Corpus n. 205.441/GO. Relator: Min. Rogerio Schietti Cruz. Julgado em 03 out. 2024b. *Diário da Justiça Eletrônico*, Brasília, 07 out. 2024.

BRASIL. Superior Tribunal de Justiça (6ª Turma). Recurso Ordinário em Habeas Corpus n. 218.358/PI. Relator: Min. Sebastião Reis Júnior. Julgado em 04 nov. 2025. *Diário da Justiça Eletrônico*, Brasília, 11 nov. 2025.

BRASIL. Superior Tribunal de Justiça (Corte Especial). Inquérito n. 1.674/DF. Relatora: Min. Nancy Andrighi. Julgado em 06 maio 2026. *Diário da Justiça Eletrônico*, Brasília, 14 maio 2026.

BRASIL. Supremo Tribunal Federal (Segunda Turma). Agravo Regimental na Ação Penal n. 1.030/DF. Relator: Min. Edson Fachin. Julgado em 25 set. 2018b. *Diário da Justiça Eletrônico*, Brasília, 18 fev. 2019.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Ação Direta de Inconstitucionalidade n. 5.527/DF. Relatora: Min. Rosa Weber. Julgado em 29 set. 2023b. *Diário da Justiça Eletrônico*, Brasília, 30 out. 2024.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Recurso Extraordinário n. 1.037.396/SP. Tema 987: Responsabilidade civil de provedores de redes sociais por conteúdo gerado por terceiros. Relator: Min. Dias Toffoli. Julgado em 26 jun. 2025d. *Diário da Justiça Eletrônico*, Brasília, 05 nov. 2025.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Recurso Extraordinário n. 1.301.250/DF. Tema 1.148: Limites para decretação judicial da quebra de sigilo de dados telemáticos em relação a pessoas indeterminadas. Relatora: Min. Rosa Weber. Julgado em 28 maio 2021d. *Diário da Justiça Eletrônico*, Brasília, 08 jun. 2021.

CONSELHO DA EUROPA. *Convenção sobre o Crime Cibernético*. Budapeste, 23 nov. 2001. (ETS n. 185). Disponível em: https://rm.coe.int/1680081561. Acesso em: 20 maio 2026.

EUROPOL. Acordo de cooperação entre a Polícia Federal brasileira e a Europol. Bruxelas, 05 mar. 2025. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2025/03/brasil-e-uniao-europeia-assinam-acordo-para-cooperacao-policial-entre-a-policia-federal-e-a-europol. Acesso em: 20 maio 2026.

FAYÃO, Vincenzo de Campos Agonilha; SILVA, Alcides Belfort. Crimes cibernéticos: a tipificação penal e os desafios na efetivação das medidas legais de combate. *Transições*, Ribeirão Preto, v. 6, n. 2, 2025. Disponível em: https://periodicos.baraodemaua.br/index.php/transicoes/article/view/1103. Acesso em: 19 maio 2026.

FERNANDES, Reicler Rosa Martins; GUIMARÃES, João Alexandre Silva Alves. Crimes virtuais e a necessidade de atualização das normas penais no combate às invasões cibernéticas. *Anima Educação*, 2025. Disponível em: https://repositorio.animaeducacao.com.br. Acesso em: 19 maio 2026.

FISBERG, Yuri. Função hash e a integridade da prova digital. *Revista Brasileira de Direito Processual Penal*, v. 11, n. 3, e1227, set./dez. 2025. Disponível em: https://doi.org/10.22197/rbdpp.v11i3.1227. Acesso em: 12 maio 2026.

GRECO, Rogério. *Curso de Direito Penal: parte especial*. 22. ed. Niterói: Impetus, 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Convenção das Nações Unidas contra o Crime Cibernético*. Adotada pela Assembleia Geral em 24 dez. 2024. Nova York: ONU, 2024. Disponível em: https://news.un.org/pt/story/2024/12/1842576. Acesso em: 20 maio 2026.

PECK, Patrícia. *Direito Digital*. 8. ed. São Paulo: Saraiva, 2023.