VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I

D597

Direito penal, processo penal e constituição I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Dani Rudnicki; Gustavo Noronha de Avila; Renata Botelho Dutra. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-171-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34

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

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I

Apresentação

O GT 61 - Direito penal, processo penal e constituição I por nós coordenado mostrou-se fiel à tradição do Conpedi de discutir, em alto nível, os temas mais atuais da pesquisa jurídica. Neste GT, em específico, todos trabalhos tiveram um compromisso com a busca e a aplicação de um direito penal e processual penal conforme com a Constituição Federal de 1988 e seus valores e princípios. Foi uma longa e profícua tarde de sábado, com muita dedicação e empenho a fim de demonstrar a qualidade da pós-graduação em Direito no país.

O primeiro estudo, da lavra de Fernando Antonio Holanda Pereira Junior, intitulado "A EXPANSÃO DOS CONSENSOS PENAIS: UMA CRÍTICA DA JUSTIÇA PENAL NEGOCIADA COMO POLÍTICA PÚBLICA CRIMINAL" trouxe uma rara e oportuna visão crítica das propostas de consensos na área do direito penal.

O trabalho de Matheus Henrique De Freitas Urgniani e Pedro Henrique Marangoni, "A FALTA DE JUSTA CAUSA PARA A AÇÃO PENAL EM RAZÃO DA VIOLAÇÃO DA CADEIA DE CUSTÓDIA", investe em discussão processual imperiosa para garantia do devido processo legal.

Sebastian Borges de Albuquerque Mello e José Henriques Mutemba apresentaram no artigo "A JUSTIÇA RESTAURATIVA NA EXECUÇÃO PENAL MOÇAMBICANA: UM MODELO ALTERNATIVO À RETRIBUIÇÃO E À PREVENÇÃO ESPECIAL NEGATIVA" não apenas uma possibilidade de repensar a execução penal, mas igualmente um pouco do sistema penal de Moçambique.

AUTÔNOMAS?” apresenta interessante discussão dogmática sobre temas que tem repercutido por demais na jurisprudência, dogmática e mídia.

A tecnologia voltou a ser analisada no texto “DEEPFAKES E AS IMPLICAÇÕES QUANTO À INTEGRALIDADE DAS PROVAS DIGITAIS NO PROCESSO PENAL BRASILEIRO” As autoras Maria Paula Matos Medeiros, Marina Quirino Itaborahy e Ana Rosa Campos debatem o status das provas digitais em meio a tantas possibilidades de falsificação.

Deise Neves Nazaré Rios Brito, em “DOLO EVENTUAL E SUBJETIVAÇÃO JUDICIAL NO BRASIL CONTEMPORÂNEO: Análise conceitual da tipicidade subjetiva à luz da teoria clássica do delito e da filosofia”, com fundamento no processo que se seguiu ao incêndio da boate Kiss no Rio Grande do Sul discorre sobre o conceito fluido de dolo eventual.

O tema da lavagem de capitais retorna no texto “ENTRE A LEGALIZAÇÃO E A ILUSÃO DE CONTROLE: uma análise crítica da lei nº 14.790/2023 no combate à lavagem de dinheiro nas apostas digitais”. Roberto Carvalho Veloso, Monique Leray Costa e Ronald Luiz Neves Ribeiro Junior debatem sobre as possibilidades e alcance da legislação neste ponto nebuloso da vida social que são as apostas agora digitais.

Em seguida, a persistente discussão do sistema acusatório foi trabalhada por Yuri Anderson Pereira Jurubeba , Fernanda Matos Fernandes de Oliveira Jurubeba e Tarsis Barreto Oliveira. Neste sentido, foi discutido, no artigo "INTERPRETAÇÃO DO ARTIGO 3º-A DO CÓDIGO DE PROCESSO PENAL SOB A ÓTICA COLEGIADA DO SUPREMO TRIBUNAL FEDERAL", a interpretação dos tribunais superiores ao desenho acusatório do processo penal brasileiro.

Rodrigo Teles de Oliveira, no trabalho "JUIZ GARANTIDOR OU JUIZ-INQUISIDOR?

Continuando, Juliana Gurjão Monteiro e Newton Torres dos Santos Cruz, em "O PROCEDIMENTO INVESTIGATÓRIO CRIMINAL NO MINISTÉRIO PÚBLICO: AS DECISÕES DO SUPREMO TRIBUNAL FEDERAL QUE AFETARAM A NATUREZA JURÍDICA DO PIC", analisam a importante questão da Investigação Preliminar feita pelo Ministério Público. O texto analisou a repercussão das Decisões Conjuntas das Ações Diretas de Inconstitucionalidade (ADIs) nº 2.943, 3.309 e 3.318, e das ADI nº 6.298, 6.299, 6.300 e 6.305, na natureza jurídica do PIC e sua condução no âmbito do MP.

Por último, Marcelo Wordell Gubert e Flavia Piccinin Paz trabalham, em visão restrita à dogmática, as provas atípicas no processo penal. A partir da epistemologia da prova penal, apresentam o impacto das tecnologias emergentes e os limites constitucionais.

Foram trabalhos importantes e que certamente contribuirão imensamente com o avanço dos temas na nossa realidade.

Desejamos uma ótima leitura!

Dani Rudnicki

Gustavo Noronha de Avila

Renata Botelho Dutra

A PERSECUÇÃO PENAL E A PROVA DIGITAL EXTRAÍDA DE DISPOSITIVOS MÓVEIS: DESAFIOS JURÍDICOS NA COLETA, PRESERVAÇÃO E ADMISSIBILIDADE PROBATÓRIA

CRIMINAL PROSECUTION AND DIGITAL EVIDENCE EXTRACTED FROM MOBILE DEVICES: LEGAL CHALLENGES IN THE COLLECTION, PRESERVATION AND ADMISSIBILITY OF EVIDENCE

Bruno Emanuel Setubal Learte [1]
Roberto Carvalho Veloso [2]
Anna Carollina de Oliveira Abreu Melo [3]

Resumo

O presente artigo tem como temática a persecução penal, desenvolvendo-se a partir da inter-relação entre provas digitais, cadeia de custódia, ilicitude probatória e técnicas de Computação Forense. Analisa-se o entendimento do Superior Tribunal de Justiça (STJ) quanto à licitude ou ilicitude de provas digitais obtidas a partir de dispositivos móveis, com base em julgados paradigmáticos divulgados por meio dos Informativos de Jurisprudência da Corte. Além disso, descrevem-se técnicas de informática forense aplicadas à obtenção, preservação, autenticação e análise de provas digitais extraídas de dispositivos móveis. Para tanto, adotou-se o método hipotético-dedutivo, associado à pesquisa bibliográfica e à análise crítica de teorias da prova e de procedimentos forenses, em comparação com os entendimentos firmados pelo STJ. Buscou-se, assim, avaliar a hipótese de que a Corte anula casos criminais com base em uma compreensão insuficiente dos fundamentos técnicos da Computação Forense. Verificou-se, ainda, que há uma lacuna entre os requisitos técnicos exigidos para a integridade e autenticidade das provas digitais e a forma como essas questões são tratadas no âmbito judicial. Ao final, concluiu-se pela confirmação da hipótese, destacando-se a necessidade de maior capacitação técnica dos operadores do direito e de uma interlocução mais consistente entre o saber jurídico e o saber tecnológico.

Palavras-chave: Segurança da informação, Validade probatória, Evidencia digital, forense digital, Processo penal

Abstract/Resumen/Résumé

The theme of this article is criminal prosecution, based on the interrelationship between digital evidence, chain of custody, evidentiary illegality and computer forensics techniques. The understanding of the Superior Court of Justice (STJ) regarding the lawfulness or unlawfulness of digital evidence obtained from mobile devices is analyzed, based on paradigmatic judgments published in the Court's case law reports. It also describes computer forensics techniques applied to obtaining, preserving, authenticating and analyzing digital evidence extracted from mobile devices. To this end, the hypothetical-deductive method was adopted, associated with bibliographical research and a critical analysis of theories of evidence and forensic procedures, in comparison with the decisions made by the STJ. The aim was to evaluate the hypothesis that the Court overturns criminal cases based on an insufficient understanding of the technical foundations of computer forensics. It was also found that there is a gap between the technical requirements for the integrity and authenticity of digital evidence and the way in which these issues are dealt with in the judicial sphere. In the end, we concluded that the hypothesis was confirmed, highlighting the need for greater technical training for legal operators and a more consistent dialogue between legal and technological knowledge.

Keywords/Palabras-claves/Mots-clés: Information security, Evidential validity, Digital evidence, Digital forensics, Criminal proceedings

1. INTRODUÇÃO

O Superior Tribunal de Justiça (STJ), no exercício de suas competências constitucionais, possui a atribuição de uniformizar a interpretação da legislação federal em âmbito nacional, nos termos do art. 105, inciso III, da Constituição Federal de 1988 (BRASIL, 1988). A persecução penal, por sua vez, é integralmente regida por normas federais, uma vez que compete privativamente à União legislar sobre Direito Penal e Direito Processual Penal, conforme dispõe o art. 22, inciso I, da mesma Carta Magna. Nessa perspectiva, os principais diplomas normativos que disciplinam a persecução penal – o Código Penal (Brasil, 1940) e o Código de Processo Penal (Brasil, 1941) – têm natureza federal.

Considerando os avanços tecnológicos e o impacto da transformação digital sobre as práticas criminosas, torna-se imprescindível examinar a jurisprudência consolidada pelo STJ, especialmente no que se refere à aplicação da legislação vigente aos delitos que envolvem a utilização de provas digitais, notadamente aquelas extraídas de dispositivos móveis, como os smartphones. Não obstante, verifica-se que a compreensão técnica das provas digitais nem sempre é adequada por parte dos ministros da Corte, o que pode ensejar equívocos graves, como a anulação indevida de processos penais fundamentada em interpretações equivocadas acerca de aspectos técnicos da Computação Forense.

Diante desse cenário, a presente pesquisa se estrutura em torno da seguinte problemática: Em que medida a ausência de conhecimento técnico em Informática Forense influencia o entendimento do Superior Tribunal de Justiça quanto à licitude das provas digitais obtidas a partir de dispositivos móveis? Para responder a essa indagação, parte-se da premissa de que a mera extração de dados de dispositivos móveis visa à preservação da prova e à manutenção da cadeia de custódia, prescindindo, portanto, de autorização judicial específica — a qual se torna exigível apenas na fase de análise do conteúdo extraído.

O objetivo geral deste estudo consiste em examinar o posicionamento do STJ acerca da licitude ou ilicitude das provas digitais obtidas a partir de dispositivos móveis, considerando três contextos distintos: (i) cumprimento de mandado judicial de busca e apreensão; (ii) apreensão decorrente de prisão em flagrante; e (iii) entrega voluntária do dispositivo. Os objetivos específicos envolvem a descrição das técnicas forenses

aplicáveis à aquisição, autenticação e análise de provas digitais extraídas de dispositivos móveis, correlacionando-as com os institutos da cadeia de custódia, da prova ilícita e do direito fundamental à prova.

Para tanto, adota-se o método hipotético-dedutivo, com base em pesquisa bibliográfica e análise crítica de teorias da prova e de práticas de Computação Forense, as quais são confrontadas com três julgados paradigmáticos do STJ, publicados nos "Informativos de Jurisprudência" – periódicos oficiais destinados à sistematização e à divulgação das principais teses jurídicas firmadas pela Corte. Como resultado, almeja-se confirmar ou refutar a hipótese de que o STJ, por deficiência técnico-científica na compreensão de elementos forenses, tem proferido decisões que anulam indevidamente ações penais fundadas em provas digitais.

2. DISPOSITIVOS MÓVEIS COMO FONTE DE PROVA DIGITAL: ANÁLISE JURISPRUDENCIAL DO STJ

A investigação criminal pode ser conceituada como o conjunto estruturado de diligências, formulações hipotéticas e análises técnicas voltadas à apuração da autoria e materialidade de uma infração penal. Trata-se de uma fase pré-processual essencial para o exercício da persecução penal, sendo orientada pelo princípio da legalidade e guiada por critérios de razoabilidade e proporcionalidade na produção de provas.

Nesse contexto, os dispositivos móveis – tais como smartphones, tablets e notebooks portáteis – constituem ferramentas tecnológicas amplamente utilizadas pela população, possuindo funções múltiplas que vão além da simples comunicação. Tais aparelhos portáteis, com capacidade de conexão à internet, são dotados de sistemas operacionais complexos, memória interna expansível, sensores de geolocalização (GPS), câmeras de alta definição, mecanismos de armazenamento em nuvem e inúmeros aplicativos voltados à comunicação instantânea, redes sociais, gerenciamento de dados e transações financeiras.

Por armazenarem vasto volume de informações pessoais e sensíveis – como registros de chamadas, mensagens de texto e voz, e-mails, arquivos multimídia, localização geográfica e histórico de navegação – os dispositivos móveis têm se consolidado como fontes relevantes de prova digital na investigação criminal contemporânea. Sua análise, contudo, demanda cuidados técnicos específicos e o respeito aos direitos fundamentais do investigado, especialmente no que tange à inviolabilidade

da intimidade, do sigilo das comunicações e à necessidade de autorização judicial para acesso ao conteúdo armazenado, conforme jurisprudência consolidada do Superior Tribunal de Justiça (STJ).

2.1 BUSCA E APREENSÃO DE DISPOSITIVOS MÓVEIS

O ordenamento jurídico brasileiro disciplina a busca e apreensão no Código de Processo Penal (CPP), mais especificamente em seu Livro I (“Do Processo em Geral”), Título VII (“Da Prova”), Capítulo XI (“Da Busca e da Apreensão”), compreendendo os artigos 240 a 250 do referido diploma legal (Brasoç, 1941). Embora a busca e a apreensão sejam tratadas de forma conjunta, tais institutos possuem significados distintos no contexto jurídico.

A busca refere-se à diligência destinada à localização de pessoas ou objetos, enquanto a apreensão consiste em uma medida de constrição que coloca tais pessoas ou objetos sob a custódia dos órgãos de persecução penal (Lopes Júnior, 2022). Assim, caso determinado objeto seja entregue voluntariamente, haverá apreensão sem necessidade de busca. O contrário também é possível: pode-se realizar diligência de busca sem êxito, ou seja, sem encontrar a pessoa ou o objeto procurado, inexistindo, portanto, a apreensão (Lima, 2020, p. 793).

Nesse contexto, Lima (2020, p. 793) afirma que a busca e apreensão não constituem meio de prova em si, mas sim meio de obtenção de prova, possuindo, assim, natureza procedimental. Por essa razão, admite-se sua realização por autoridades que não o magistrado, como os agentes policiais. Ademais, a leitura do art. 240 do CPP (Brasil, 1941) demonstra, de forma clara e exemplificativa, que uma das finalidades da busca é a obtenção de elementos necessários à comprovação da infração penal e à elucidação dos fatos investigados.

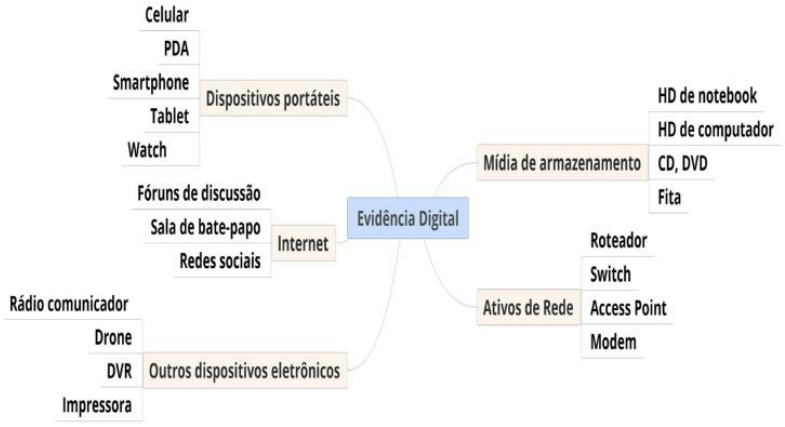
O art. 242 do CPP (Brasil, 1941) dispõe que a busca pode ser realizada de ofício ou a requerimento de qualquer das partes. Sobre esse ponto, Lima (2020, p. 794) diferencia a busca pessoal da busca domiciliar. Conforme o art. 6º, inciso II, do CPP, tendo a autoridade policial conhecimento da infração penal, deve apreender os objetos relacionados ao fato criminoso, após a liberação pelos peritos. Nesse caso, a autoridade policial atua de ofício, sendo dispensável autorização judicial prévia – hipótese comum nas buscas pessoais, como as realizadas no contexto de prisões em flagrante, quando se visa identificar e apreender objetos de interesse à persecução penal.

Por outro lado, considerando o princípio da inviolabilidade do domicílio, previsto no art. 5º, inciso XI, da Constituição Federal (Brasil, 1988), a busca domiciliar somente é admissível mediante mandado judicial expedido por autoridade competente, respeitando-se as regras do juiz natural (Lima, 2020, p. 794).

O art. 240 do CPP (Brasil, 1941) apresenta um rol exemplificativo de pessoas e objetos passíveis de busca e apreensão (Lima, 2020, p. 795). Destacam-se, nesse rol, as alíneas “f” e “h” do §1º, que autorizam, respectivamente, a apreensão de cartas – abertas ou não – destinadas ao acusado ou sob sua posse, quando houver suspeita de que seu conteúdo possa contribuir para a elucidação do fato, bem como a coleta de qualquer elemento de convicção.

Considerando que o CPP foi originalmente redigido na década de 1940, quando inexistiam diversas tecnologias atualmente disponíveis, mostra-se acertada a decisão legislativa de conferir caráter exemplificativo ao rol contido no art. 240. Tal previsão permite a aplicação do instituto também às provas digitais, obtidas por meio de dispositivos móveis. É notório, inclusive, o reconhecimento, por parte do próprio Poder Judiciário, da prova digital como instrumento válido para a comprovação e elucidação de fatos.

Nesse sentido, conforme *National Institute of Justice* (2007) evidência digital é qualquer informação de valor probatório que seja armazenada ou transmitida em formato digital. Os tipos de evidências digitais aumentam continuamente. A Figura 1 organiza-as em grupos, de acordo com a similaridade dos exames necessários. Uma lista não exaustiva de evidências digitais é apresentada podem ser classificadas em:



Fonte: Elaboração própria, 2025

- Físicas: computadores (servidores, desktops, laptops), HDs externos, pen drives, MP3 players, CDs, DVDs, celulares, câmeras digitais, videogames, entre outros;
- Lógicas ou demonstrativas: dados, arquivos, textos, imagens, vídeos, músicas, e-mails, entre outros armazenados em suportes eletrônicos, ópticos ou magnéticos.

O smartphone é um acessório inseparável hoje em dia para todos. É equipado com todos os tipos de tecnologia para registrar fotos, conversas, navegações de internet, notas, chamadas e localizações, dentre outros, conforme detalhado pelo *Internacional Data Corporation* (2018). Todo o tipo de interação e movimento pode ser recolhido a partir de um smartphone pessoal. Isso pode explicar o quão valioso é essa evidência digital e os cuidados necessários para coletá-la. Se o smartphone não estiver devidamente desligado e todos os tipos de redes não estiverem desconectados, é possível que todas as informações possam ser apagadas antes mesmo de chegar ao laboratório forense (NIJ, 2008).

No que se refere aos dispositivos móveis, como os smartphones, a jurisprudência do Superior Tribunal de Justiça (STJ) entende ser lícito o acesso aos dados armazenados nesses aparelhos pelos órgãos de persecução penal, desde que em decorrência do cumprimento de mandado judicial de busca e apreensão. Tal entendimento fundamenta-se no argumento de que esse meio de obtenção de prova não se submete à Lei nº 9.296/1996 (Brasil, 1996), tampouco viola o art. 5º, inciso XII, da Constituição Federal (Brasil, 1988), conforme decidido no Recurso em *Habeas Corpus* nº 75.800-PR (Cavalcante, 2022, p. 1).

Isso porque, segundo o STJ, a interceptação de comunicações, nos termos da Constituição e da Lei nº 9.296/1996, ocorre apenas quando há comunicação em andamento, não se aplicando a dados armazenados, cuja existência decorre da liberalidade do usuário, que optou por não os excluir (Cavalcante, 2022, p. 3).

Ainda que se invoque o art. 7º da Lei nº 12.965/2014, o Marco Civil da Internet (Brasil, 2014), que garante a inviolabilidade e o sigilo das comunicações privadas armazenadas, não se configura ilicitude probatória no acesso aos dados, desde que este decorra do cumprimento de ordem judicial de busca e apreensão (Cavalcante, 2022, p. 4).

Portanto, em síntese, o STJ entende que o acesso aos dados de dispositivos móveis é lícito quando fundado em mandado judicial de busca e apreensão. No entanto, importa ressaltar que o Tribunal não distingue, sob o ponto de vista da Computação

Forense, o conceito técnico de “acesso”, tratando-o de forma genérica, o que pode gerar implicações relevantes no contexto do processo penal.

2.2 A UTILIZAÇÃO DE DADOS EXTRAÍDOS DE DISPOSITIVOS MÓVEIS APREENDIDOS EM RAZÃO DE PRISÃO EM FLAGRANTE DELITO

A prisão em flagrante é um instituto do direito processual penal que funciona como meio de defesa da própria sociedade diante do cometimento de uma infração penal (crime ou contravenção), seja de forma concomitante ou logo após a sua ocorrência. Tal instituto se divide em quatro momentos distintos: captura, condução coercitiva, lavratura do auto de prisão em flagrante e recolhimento à prisão (Lima, 2020, p. 1028). O elevado grau de certeza quanto à prática do delito justifica a prisão do indivíduo sem a prévia autorização da autoridade judiciária competente, sempre em respeito à garantia fundamental prevista no art. 5º, inciso LXI, da Constituição Federal (Brasil, 1988) (Lima, 2020, p. 1027).

Além de sua função repressiva, a prisão em flagrante também favorece a investigação penal, permitindo que os órgãos de persecução penal tenham contato direto com os vestígios deixados pela dinâmica delituosa, o que torna o procedimento investigativo mais eficiente e célere (Lima, 2020, p. 1028). As hipóteses de cabimento da prisão em flagrante estão expressamente previstas nos incisos I a IV do art. 302 do Código de Processo Penal (CPP) (Lopes Júnior, 2022).

Com base nesses dispositivos, a doutrina classifica o flagrante em diversas espécies:

a) Flagrante próprio, perfeito, real ou verdadeiro: ocorre quando o agente está cometendo a infração penal ou acaba de cometê-la, conforme previsto nos incisos I e II do art. 302 do CPP (Brasil, 1941).
b) Flagrante impróprio, imperfeito, irreal ou quase-flagrante: verifica-se quando o agente é perseguido logo após cometer a infração, sendo capturado em razão de circunstâncias que indicam sua autoria, nos termos do inciso III do art. 302 do CPP.
c) Flagrante presumido, ficto ou assimilado: difere do flagrante impróprio por não exigir perseguição, bastando que o agente seja encontrado, logo após o crime, com instrumentos, armas, objetos ou papéis que façam presumir ser ele o autor do fato, conforme o inciso IV do art. 302 do CPP (Lima, 2020, p. 1033-1034).

d) Flagrante preparado, provocado, crime de ensaio, delito de experiência ou delito putativo por obra do agente provocador: é ilícito, pois há induzimento do agente à prática delitiva por parte dos órgãos de persecução, configurando crime impossível. O Supremo Tribunal Federal (STF) consolidou esse entendimento na Súmula nº 145: "Não há crime, quando a preparação do flagrante pela polícia torna impossível a sua consumação" (Brasil, 1963).
e) Flagrante forjado, fabricado, maquinado ou urdido: é ainda mais grave, pois envolve a criação artificial de provas de um crime inexistente por policiais ou particulares, com o objetivo de legitimar falsamente uma prisão (Lima, 2020, p. 1039).
f) Flagrante esperado: é considerado lícito, pois o Estado apenas aguarda o cometimento espontâneo do crime para efetuar a prisão, sem incitar ou provocar a ação criminosa (Lima, 2020, p. 1035-1036).
g) Flagrante prorrogado, protelado, retardado ou diferido (também denominado ação controlada ou entrega vigiada): caracteriza-se pelo retardamento deliberado da intervenção policial, com o objetivo de melhor colher provas ou intervir no momento mais adequado sob a perspectiva investigativa. A ação controlada exige prévia comunicação ao juízo competente, conforme disposto no art. 8º, §1º, da Lei nº 12.850/2013, que trata das organizações criminosas (Brasil, 2013).

No que tange ao acesso a dispositivos móveis apreendidos durante a prisão em flagrante, o Superior Tribunal de Justiça (STJ) considera ilícito qualquer acesso ao conteúdo desses aparelhos sem prévia autorização judicial, conforme decidido no julgamento do Recurso em *Habeas Corpus* (RHC) nº 51.531-RO (Brasil, 2016). Por exemplo, não é permitido à polícia acessar mensagens ou conversas armazenadas em um smartphone apreendido com o autuado sem que haja autorização expressa do magistrado competente.

Esse entendimento fundamenta-se nas garantias constitucionais da inviolabilidade da intimidade, do sigilo de correspondência, dos dados e das comunicações telefônicas, previstas nos incisos X e XII do art. 5º da Constituição Federal (Brasil, 1988). Assim, a autoridade policial deve apenas apreender o celular e requisitar autorização judicial para ter acesso ao seu conteúdo (Cavalcante, 2016, p. 26). Importante destacar, ainda, que a leitura integral do julgado no RHC nº 51.531-RO revela o uso

indistinto de termos como “acesso”, “extração”, “obtenção” e “perícia”, embora esses conceitos possuam distinções relevantes sob a ótica da Informática Forense.

2.2 ENTREGA VOLUNTÁRIA DE DISPOSITIVOS MÓVEIS PELA VÍTIMA AOS ÓRGÃOS DE PERSECUÇÃO PENAL

Em 2017, o Superior Tribunal de Justiça (STJ) julgou o Recurso em *Habeas Corpu*s (RHC) nº 86.076-MT (Brasil, 2017), cuja decisão teve grande repercussão nos casos envolvendo a análise de provas obtidas por meio de dispositivos móveis. Como mencionado anteriormente, o entendimento predominante do STJ é o de que o acesso aos dados contidos em dispositivos móveis, em regra, exige autorização judicial, seja em casos de apreensão do aparelho durante flagrante delito, seja mediante o cumprimento de mandados de busca e apreensão.

No entanto, a decisão proferida no referido RHC considerou legítima a perícia realizada pela polícia em um aparelho celular sem autorização judicial, sob a justificativa de que o proprietário do dispositivo — a vítima — havia falecido, e o telefone foi entregue espontaneamente à autoridade policial por sua esposa (Cavalcante, 2017, p. 1).

A distinção essencial nesse caso diz respeito à titularidade do dispositivo móvel: se pertence à vítima ou ao investigado. Quando o aparelho é de propriedade do investigado, a autorização judicial é imprescindível em qualquer hipótese, exceto nos casos em que há mandado judicial de busca e apreensão, abrangendo expressamente os dados armazenados no dispositivo. Assim, permanece a necessidade de observância à cláusula de reserva de jurisdição.

Por outro lado, quando o dispositivo pertence à vítima, parte-se do pressuposto de que há interesse dela — ou de seus representantes — na elucidação do crime. Nas palavras de Cavalcante (2017, p. 4), tal interpretação fundamenta-se na ausência de "violação à intimidade do investigado, titular de garantias no processo penal". Em outras palavras, o Direito Processual Penal tem por objetivo, de um lado, proteger os direitos e garantias fundamentais do suspeito, investigado, indiciado, acusado ou réu; de outro, busca punir o delito e resguardar os interesses da vítima e, de forma secundária, da sociedade — considerando a função pacificadora do Direito.

Portanto, para o STJ, a autorização judicial é, em regra, dispensável para o acesso a dados de dispositivos móveis pertencentes à vítima do delito. Contudo, esse entendimento deve ser aplicado com cautela, considerando as particularidades de cada

caso concreto. O caso paradigmático analisado pela Corte Superior envolvia um crime de homicídio consumado, no qual a vítima já estava morta, e um familiar, interessado na resolução do crime, entregou espontaneamente o celular da vítima à polícia para utilização em investigação.

Em contrapartida, em situações que envolvem homicídio tentado ou outros crimes em que a vítima esteja viva e em plena consciência, entende-se que o acesso ao conteúdo de seus dispositivos móveis ainda exige ordem judicial — salvo nos casos em que a própria vítima entrega voluntariamente o aparelho à autoridade policial. Nessa hipótese, configura-se uma renúncia, ainda que tácita, ao seu sigilo de dados.

Por fim, cabe destacar que, mais uma vez, o STJ utilizou os termos "extração" e "acesso" de forma tecnicamente imprecisa, sob a perspectiva da Ciência da Computação e da Computação Forense.

3. PROVAS DIGITAIS NO CONTEXTO DA PROVA EM SENTIDO AMPLO: ASPECTOS TEÓRICOS E PRÁTICOS

Segundo Dallagnol (2018), a prova consiste em uma inferência racional que correlaciona evidências e hipóteses. O autor ensina que aquilo que é popularmente conhecido como “prova” é, tecnicamente, denominado “evidência” sob a ótica epistemológica. O percurso realizado pelo raciocínio humano entre a evidência e a hipótese é a inferência racional — ou seja, a própria prova (Badaró, 2019).

Em síntese: a evidência é o vestígio materialmente deixado na realidade; a hipótese é a possível causa que originou tal vestígio; e a inferência é o raciocínio que conecta, por meio de uma explicação, a evidência à hipótese, comprovando, assim, algo (Badaró, 2019). É importante destacar que a hipótese é, em regra, indissociável da inferência, pois uma pressupõe e fundamenta a outra. Afinal, não se pode falar em raciocínio abstrato sem hipóteses, tampouco em hipóteses sem inferências — isto é, sem “caminhos” racionais.

Nesse contexto, insere-se o conceito de “dúvida razoável” ou o adágio latino in dubio pro reo, que expressa o princípio do Direito Processual Penal segundo o qual o réu deve ser absolvido quando houver dúvida razoável quanto ao seu envolvimento no crime ou mesmo sobre a existência do próprio delito.

Dallagnol (2018) propõe que, com base na tríade "evidência, hipótese e inferência", os casos penais devem ser conduzidos por um standard probatório mínimo

fundamentado na chamada “inferência para a melhor explicação” (IME). A IME consiste na adoção da hipótese que, à luz da experiência humana (background de crenças empíricas), melhor explica um determinado conjunto de provas (Dallagnol, 2018, p. 25).

Tome-se como exemplo a apreensão de um smartphone cuja memória contém mensagens de texto que mencionam a comercialização de “pneus” — essa é a primeira evidência. No entanto, a apreensão ocorreu no âmbito de uma investigação sobre tráfico de drogas. Surge, então, o questionamento: qual a relação entre pneus e drogas? A primeira hipótese é a de que os traficantes aproveitam a logística do tráfico para contrabandear pneus. Por outro lado, caso se descubra — por meio de uma segunda evidência — que “pneu” é um código para “cocaína”, passa-se a considerar a hipótese de que todas as mensagens se referem, na verdade, à venda de drogas.

Desse modo, considerando o contexto das investigações e o conteúdo das mensagens, deve-se adotar a hipótese que, acima de qualquer dúvida razoável, melhor explica o caso concreto por meio de inferências racionais (Dallagnol, 2018). A IME, portanto, serve como base para a construção do conhecimento utilizado na tomada de decisões pelos operadores do Sistema de Justiça Criminal. É com base nela que o magistrado decidirá pela absolvição ou condenação do réu.

Transpondo esses conceitos do campo jurídico para o mundo digital, pode-se estabelecer uma analogia entre as tríades “evidência, hipótese e inferência”, do Direito Processual, e “dado, informação e conhecimento”, da Ciência da Computação. Para compreender essa equivalência, é necessário compreender os significados técnicos desses termos na área da Computação.

Segundo Boff, Fortes e Freitas (2018), dados são símbolos ou signos brutos, sem significado relacional, que representam uma parcela da realidade, passada ou presente. Por exemplo, “azul” é um dado que remete a uma cor, mas não se relaciona diretamente a algo ou alguém. Informação, por sua vez, consiste no significado objetivo obtido a partir da correlação entre dados, com semântica (Boff; Fortes; Freitas, 2018). Se correlacionarmos os dados “azul”, “mar” e “água”, por exemplo, obtemos a informação de que “a água do mar é da cor azul”.

O conhecimento, por fim, é o resultado da síntese obtida a partir de reflexões destinadas à tomada de decisões. No exemplo citado, um indivíduo pode decidir mergulhar no mar por entender que ele não está poluído, com base na informação de que sua água é azul e na crença empírica de que “mar azul significa que ele está limpo”.

Dessa forma, observa-se uma equivalência técnica entre as tríades analisadas: evidência corresponde a dado; hipótese, à informação; e inferência, ao conhecimento. Conclui-se, então, que o dado é a base de toda análise probatória no contexto das provas digitais.

Para conceituar prova digital, é necessário compreender a área denominada Computação Forense ou Forense Computacional (*Computer Forensics*), que envolve a extração, identificação, preservação e documentação de evidências digitais a partir de dados e informações armazenados em mídias magnéticas, ópticas ou eletrônicas (Craiger, 2007). A Computação Forense pode ser entendida como uma peça do quebra-cabeça investigativo. Assim, provas digitais são evidências digitais que podem ser coletadas e analisadas por meio de métodos e técnicas específicas da Computação Forense, com o objetivo de formular hipóteses e obter inferências válidas.

De acordo com Kruse & Heiser (2002), os procedimentos forenses aplicáveis às provas digitais podem ser sintetizados pelo mnemônico dos "3 A's":

Adquirir as evidências sem alterar ou danificar o original;

Autenticar que as evidências recuperadas são idênticas aos originais;

Analisar os dados sem modificá-los.

Segundo a Publicação Especial 800-101 do NIST (2007), a chave para o sucesso na análise forense de dispositivos móveis está na compreensão de suas características de hardware e software. Os dados dos assinantes e suas atividades, acessados por meio dos celulares, são frequentemente fontes valiosas de provas.

A maioria dos dispositivos móveis compartilha um conjunto básico de componentes: microprocessador, memória ROM, memória RAM, módulo de rádio, processador de sinal digital, alto-falante, tela, sistema operacional, bateria, GPS, câmera, entre outros.

De modo semelhante, Eleutério & Machado (2010, p. 94-99) descrevem quatro fases nos exames periciais de dispositivos móveis:

Preservação – busca preservar tanto o equipamento quanto as evidências nele contidas;

Extração – consiste na coleta efetiva das evidências digitais, abrangendo dados como chamadas, mensagens de texto, imagens, vídeos, entre outros, além dos metadados. Nesta fase, realiza-se a cópia eletrônica bit a bit do conteúdo, por meio de técnicas conhecidas como "imagem" (Kruse & Heiser, 2002) ou "espelhamento" (Eleutério & Machado, 2010, p. 55). É fundamental assegurar a integridade e

autenticidade das provas extraídas, pois servirão como base para o processo judicial. Para isso, utilizam-se ferramentas forenses (*hardware e software*) e dispositivos como *write blockers*, que impedem a escrita no equipamento original durante o processo;

Análise – consiste no exame detalhado dos dados extraídos, visando identificar evidências digitais relacionadas ao crime investigado (Eleutério & Machado, 2010, p. 65);

Formalização – refere-se à elaboração do laudo pericial, que deve apresentar detalhadamente os procedimentos adotados e responder aos quesitos propostos (Eleutério & Machado, 2010, p. 70).

É essencial que a extração e análise das evidências digitais reproduzam a forma como o usuário acessava ou interagia com o dispositivo. Deve-se lembrar que as evidências lógicas derivam de evidências físicas e que as provas digitais precisam de suporte físico para existir. Portanto, a conexão entre evidências físicas e lógicas é fundamental para sustentar juridicamente a relação entre os suportes materiais e digitais (Freitas, 2009).

4. CADEIA DE CUSTÓDIA E PROVAS ILÍCITAS: A PROTEÇÃO DO DIREITO FUNDAMENTAL À PROVA NO ESTADO DEMOCRÁTICO DE DIREITO

Lima (2020, p. 718) define cadeia de custódia como um "mecanismo garantidor da autenticidade das evidências coletadas e examinadas, assegurando que correspondem ao caso investigado, sem que haja lugar para qualquer tipo de adulteração". Em outras palavras, trata-se de um procedimento que permite rastrear a prova desde sua origem até sua apresentação no processo judicial, de forma cronológica e concatenada. Esse procedimento possibilita que acusação, defesa e o juízo verifiquem se o conjunto probatório é autêntico ou se há indícios de manipulação, como a inserção de provas forjadas com a intenção de incriminar ou absolver.

De acordo com Lopes Júnior (2022, p. 1036), "a cadeia de custódia exige o estabelecimento de um procedimento regrado e formalizado, documentando toda a cronologia existencial daquela prova, para permitir a posterior validação em juízo e exercício do controle epistêmico". Uma eventual quebra na cadeia de custódia pode acarretar a nulidade de todo um processo criminal (Lopes Júnior, 2022, p. 1043), especialmente diante da possibilidade de contaminação das demais provas por derivação.

No caso específico das provas digitais, há ainda maior fragilidade, já que essas podem ser danificadas acidental ou intencionalmente, especialmente quanto à (FERREIRA, 1963):

a) ocultação: ato de esconder, disfarçar ou dissimular informações;

b) obliteração: destruição completa, sem deixar vestígios;

c) adulteração: falsificação ou corrupção de dados.

Para melhor compreensão da cadeia de custódia, é necessário discutir o conceito de provas ilícitas. O artigo 5º, inciso LVI, da Constituição Federal (Brasil, 1988) estabelece o direito fundamental à prova, ao afirmar que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos".

No campo do Direito Processual Penal, Lima (2020, p. 685) afirma que a vedação das provas ilícitas atua como instrumento de controle da regularidade da persecução penal, inibindo práticas probatórias ilegais. Assim, prioriza-se a eficiência processual ainda que isso implique em eventuais absolvições, uma vez que o contrário poderia conduzir a condenações injustas, mais gravosas para o sistema.

Ditados populares como “os fins não justificam os meios” e “melhor absolver um culpado do que condenar um inocente” ajudam a ilustrar a lógica subjacente à inadmissibilidade das provas ilícitas. Segundo Lima (2020), a prova ilegal é gênero do qual derivam duas espécies: a prova ilícita e a ilegítima. A primeira decorre da violação de normas de direito material, como a confissão obtida mediante tortura. Já a segunda resulta da inobservância de normas processuais, como ocorre, por exemplo, quando uma prova é exibida aos jurados no Tribunal do Júri sem ter sido previamente juntada aos autos com a antecedência mínima de três dias, conforme exige o artigo 479 do Código de Processo Penal (CPP) (Lima, 2020).

Lima (2020) também reconhece que uma mesma prova pode ser considerada ilegal por violar simultaneamente normas de direito material e processual. Um exemplo é a obtenção de provas digitais por meio da invasão domiciliar noturna de um investigado, sem mandado judicial, com a apreensão de seu celular e posterior uso de mensagens extraídas no inquérito policial.

Nessa situação, há violação de normas processuais relativas à busca e apreensão, e também de direito material, configurando o crime de abuso de autoridade previsto no art. 22, §1º, III, da Lei nº 13.869/2019 (Brasil, 2019), que proíbe buscas domiciliares após as 21h ou antes das 5h.

Diante da apresentação dos conceitos de cadeia de custódia e de prova ilegal (ilícita e ilegítima), cabe agora correlacioná-los, visando à compreensão de sua aplicação à obtenção de provas digitais em dispositivos móveis. Nesse cenário, é fundamental abordar a chamada prova ilícita por derivação, prevista no artigo 157 do CPP, inspirada na doutrina norte-americana conhecida como "*fruit of the poisonous tree*" ("fruto da árvore envenenada"), originária do caso *Silverthorne Lumber Co. v. United States*, julgado pela Suprema Corte dos EUA em 1920 (Carvalho, 2014).

Naquele caso, discutiu-se a possibilidade de o Estado utilizar cópias de livros contábeis apreendidos ilegalmente para processar empresas por sonegação fiscal. A Corte decidiu que tais cópias não poderiam ser utilizadas, uma vez que derivavam de provas originalmente ilícitas. Ou seja, a "árvore" estava envenenada pela ilegalidade da apreensão, contaminando seus "frutos" – as cópias. Assim, tudo o que for produzido a partir de uma prova ilegal deve ser desentranhado dos autos (Estados Unidos Da América, 1920).

Contudo, há exceções. O §1º do art. 157 do CPP admite o uso de provas derivadas de ilícitas quando não houver nexo de causalidade entre elas ou quando for possível obtê-las de forma independente. Segundo o §2º do mesmo artigo, fontes independentes são aquelas que, por meios regulares e usuais de investigação, poderiam conduzir aos mesmos fatos objeto da prova.

Portanto, a cadeia de custódia desempenha papel fundamental na verificação da origem das provas, permitindo sua auditoria jurídica e aferição de legalidade, ilicitude ou ilegitimidade. Dada sua importância, o legislador tratou do tema nos artigos 158-A a 158-F do CPP. No entanto, esses dispositivos legais não contemplam de forma específica os vestígios digitais. Para suprir essa lacuna, são utilizados procedimentos tecnológicos que garantem que a prova digital seja auditável e detenha características como integridade, rastreabilidade, autenticidade, veracidade, confiabilidade, legalidade, transparência e idoneidade — tornando-a, assim, lícita e legítima.

Na Computação Forense, a integridade dos dados refere-se à garantia de que os dados não foram adulterados, destruídos ou modificados durante as etapas de preservação, extração ou análise.

Em conformidade com o art. 169, parágrafo único, do CPP, os peritos devem registrar no laudo qualquer alteração no estado das coisas e discutir, no relatório, as consequências dessas alterações para a dinâmica dos fatos. Assim, cabe a peritos e demais

profissionais garantir e preservar a integridade das evidências, digitais ou não, sob pena de invalidação da prova.

A integridade das evidências digitais é garantida por ferramentas que aplicam criptografia com a geração de códigos *hash*. Conforme explica Freitas (2008), a função *hash* tem por objetivo gerar uma sequência alfanumérica única para cada conjunto de dados, com base no conteúdo do próprio documento. Dessa forma, qualquer modificação, por menor que seja, resultará em um *hash* diferente. Assim, a simples comparação dos valores de hash de dois arquivos permite verificar sua autenticidade: apenas documentos com *hashes* idênticos são idênticos em conteúdo.

Dessa forma, a cadeia de custódia, aliada à criptografia e à geração de *hash*, constitui procedimento essencial para resguardar o direito fundamental à prova, preservando sua autenticidade, integridade e demais propriedades legais e técnicas. Esse conjunto de medidas é fundamental para evitar que ilicitudes contaminem as evidências digitais.

É com base nesse arcabouço teórico e legal que se propõe, a seguir, a análise da hipótese de que o Superior Tribunal de Justiça (STJ) vem anulando indevidamente casos criminais por desconhecimento técnico em Computação Forense.

Busca-se avaliar se a jurisprudência atual do STJ leva em consideração as particularidades técnicas relacionadas ao manuseio de provas digitais, e se as decisões proferidas têm se revelado equivocadas em virtude dessa deficiência. Afinal, como mencionado, a legislação vigente ainda não disciplina expressamente a cadeia de custódia no contexto digital.

6. Considerações Finais

É recorrente a constatação de que o Superior Tribunal de Justiça (STJ), ao julgar casos que envolvem provas digitais, frequentemente não distingue com precisão os termos técnicos da área da Computação Forense. Essa deficiência conceitual tem levado, por vezes, à anulação indevida de processos penais, especialmente quando se considera, equivocadamente, que a mera extração de dados de dispositivos eletrônicos equivale à sua análise de conteúdo. Tal confusão compromete a compreensão jurídica sobre a regularidade da produção de prova digital no âmbito investigativo.

Sob a ótica técnico-científica da Computação Forense, é essencial a adoção do mnemônico dos “3 A’s” — aquisição, autenticação e análise de evidências — como base para o correto entendimento do fluxo de tratamento de provas digitais. Cada uma dessas etapas cumpre uma função distinta e essencial dentro da cadeia de custódia. A aquisição consiste na coleta dos dados digitais presentes no dispositivo eletrônico; a autenticação garante que os dados extraídos são íntegros e não foram alterados; e a análise, por fim, corresponde à interpretação do conteúdo dos dados, com o objetivo de obter informações relevantes à elucidação do fato criminoso.

Nesse sentido, a nulidade probatória somente pode ser reconhecida quando a análise dos dados — que implica acesso ao conteúdo e inferência de informações sensíveis — ocorre sem autorização judicial, violando o direito à intimidade e à privacidade do investigado, nos termos do art. 5º, X e XII da Constituição Federal. Em contrapartida, as etapas de aquisição e autenticação podem, e devem ser realizadas de ofício pelos órgãos de persecução penal (autoridades policiais e peritos), como forma de preservar a integridade da prova digital e assegurar a fidedignidade de sua cadeia de custódia, nos moldes exigidos pela Lei nº 13.964/2019 (Pacote Anticrime).

A correta distinção entre essas fases é fundamental, sobretudo para garantir a auditabilidade da prova digital, ou seja, a possibilidade de que todas as ações praticadas sobre o material probatório possam ser verificadas e reconstituídas por especialistas, inclusive pela defesa técnica. A ausência de procedimentos técnicos padronizados compromete não apenas a admissibilidade da prova, mas também o contraditório e a ampla defesa.

De forma didática, pode-se traçar um paralelo entre a extração de dados digitais e a apreensão de projéteis em um local de homicídio: ambos são atos de preservação da materialidade da prova. Já a análise forense dos dados extraídos, tal como a comparação balística entre projéteis e a arma apreendida com o suspeito, é um procedimento investigativo que exige autorização judicial prévia, por adentrar no conteúdo informacional.

Além disso, é importante destacar que a jurisprudência ainda carece de uniformidade e sensibilidade técnica ao tratar de provas digitais, sendo notável o desconhecimento de terminologias como *imaging, hashing, volatility, live forensics*, entre outras. Essa lacuna tem repercussões práticas sérias: a anulação de provas digitalmente obtidas de forma correta e legal, apenas por não se compreenderem os limites e as garantias de cada fase do processo forense.

Portanto, fica evidenciado que a falta de domínio técnico sobre os procedimentos da Computação Forense por parte dos tribunais superiores, em especial o STJ, pode ensejar a invalidação indevida de provas digitais e, por consequência, comprometer investigações legítimas e o regular exercício da jurisdição penal. Torna-se urgente, nesse cenário, a capacitação técnica continuada de magistrados e membros do Ministério Público, bem como a institucionalização de protocolos forenses nacionais, para assegurar segurança jurídica, proteção de direitos fundamentais e a efetividade da persecução penal em tempos digitais.

7. REFERÊNCIAS

BADARÓ, Gustavo Henrique. **Epistemologia jurídica e prova penal**. São Paulo: Thomson Reuters Brasil, 2019.

BRASIL. **Constituição da República Federativa do Brasil, 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.html. Acesso em: 12 abr. 2025.

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Brasília, 7 dez. 1940. em: http://www.planalto.gov.br/ccivil_03/decretolei/del2848compilado.htm. Acesso em: 12 abr. 2025. out. 1941.

BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Brasília, 3 Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/del3689compilado.htm. Acesso em: 10 abr. 2025.

BRASIL. Lei nº 12.850, de 2 de agosto de 2013. **Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995**; e dá outras providências, 2 ago. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 10 abr. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 abr. 2025.

BRASIL. **Lei nº 13.869, de 5 de setembro de 2019. Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de**

julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), 5 set. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm. Acesso em: 10 abr. 2025.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. **Regulamenta o inciso XII, parte final, do art. 5° Federal, 24 jul. 1996**. Disponível http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 10 abr. 2025.

BRASIL. **Superior Tribunal de Justiça**. Recurso em Habeas Corpus nº 51.531/RO – Rondônia. Relator: Ministro Néfi Cordeiro, Sexta Turma, julgado em 19/4/2016, DJe de 9/5/2016. Jurisprudência do STJ. Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e +@num=%2751531%27)+ou+(%27RHC%27+adj+%2751531%27).suce.)&thesaurus=JURI DICO&fr=veja. Acesso em: 14 abr. 2025.

BRASIL. **Superior Tribunal de Justiça**. Recurso em Habeas Corpus nº 86.076/MT – Mato Grosso. Relator: Ministro Sebastião Reis Júnior, relator para acórdão Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 19/10/2017, DJe de 12/12/2017. Jurisprudência do STJ. Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e +@num=%2786076%27)+ou+(%27RHC%27+adj+%2786076%27).suce.)&thesaurus=JURI DICO&fr=veja. Acesso em: 13 abr. 2025.

BRASIL. **Superior Tribunal de Justiça**. Recurso em Habeas Corpus nº 75.800/PR – Paraná. Relator: Ministro Felix Fischer, Quinta Turma, julgado em 15/9/2016, DJe de 26/9/2016. Jurisprudência do STJ. Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e +@num=%2775800%27)+ou+(%27RHC%27+adj+%2775800%27).suce.)&thesaurus=JURI DICO&fr=veja. Acesso em: 10 abr. 2025.

BRASIL. **Supremo Tribunal Federal**. Súmula nº 145. In: _____. Aplicação das Súmulas no STF. Brasília, 1963. Disponível em: https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=30&sumula=2119#:~:text=N %C3%A3o%20h%C3%A1%20crime%2C%20quando%20a,torna%20imposs%C3%ADvel% 20a%20sua%20consuma%C3%A7%C3%A3o. Acesso em: 10 abr. 2025.

CARVALHO, Luis Gustavo Grandinetti Castanho de. **Processo Penal e Constituição: princípios constitucionais do processo penal**. São Paulo: Editora Saraiva, 2014. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502224308/. Acesso em: 12 abr. 2025.

CAVALCANTE, Márcio André Lopes. É lícito o acesso aos dados armazenados em celular apreendido com base em autorização judicial. **Buscador Dizer o Direito**, 2016, Manaus. Disponível em:

<https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/5c3b99e8f92532e5ad 1556e53ceea00c>. Acesso em: 12 abr. 2025.

CAVALCANTE, Márcio André Lopes. Informativo esquematizado: Informativo 583-STJ. **Dizer Direito**, 2016, Manaus. Disponível em: <https://dizerodireitodotnet.files.wordpress.com/2016/07/info-583-stj1.pdf>. Acesso em: 12 abr. 2025.

CAVALCANTE, Márcio André Lopes. Mesmo sem autorização judicial, polícia pode acessar conversas do Whatsapp da vítima morta, cujo celular foi entregue pela sua esposa. **Buscador dizer o Direito**, 2017, Manaus. Disponível <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/211b39255232ab59c e78f2e28cd0292b> Acesso em: 12 abr. 2025.

CRAIGER, John Philip. **Computer forensics procedures and methods**. To appear in H. Bigdoli (Ed.), Handbook of Information Security. John Wiley & Sons, 2007.

DALLAGNOL, Deltan Martinazzo. **As lógicas das provas no processo: prova direta, indícios e presunções**. Porto Alegre: Livraria do Advogado, 2018. 362 p.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a computação forense**. São Paulo: Novatec Editora, 2010.

ESTADOS UNIDOS DA AMÉRICA. **Supreme Court of the United States. Silverthorne Lumber Company, Inc., et al. v. United States. Relator: Judge Oliver Wendell Holmes Jr**. Washington, D.C., 26 de janeiro de 1920. HeinOnline. Disponível em: < https://heinonline.org/HOL/P?h=hein.usreports/usrep251&i=425 >. Acesso em: 14 abr. 2025.

FERREIRA, Aurélio Buarque de Hollanda. **Pequeno Dicionário Brasileiro da Língua Portuguesa**, 10ª Edição, Editora Civilização Brasileira S.A., Rio de Janeiro, 1963.

FREITAS, Cinthia Obladen de Almendra. Assinatura Digital: necessidade ou obrigação? In EFING, Antônio Carlos; FREITAS, Cinthia Obladen de Almendra (Orgs.). **Direito e questões tecnológicas: aplicados no desenvolvimento social.** Curitiba, PR: Juruá, 2008.

FREITAS, Cinthia Obladen de Almendra. Procedimentos Técnicos e Jurídicos para a Produção Antecipada de Provas Digitais. In: I Congresso de Computação Forense, 2009, São Paulo. **Anais do I Congresso de Computação Forense**. São Paulo: Univ. Presbiteriana Mackenzie, 2009. v. 1. p. 1-10.

KRUSE, Warren G.; HEISER, Jay G. **Computer forensics: incident response essentials**. Indianapolis: Addison-Wesley, 2002.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**: Volume Único. 8. ed. rev. atual. e aum. Salvador: Juspodivm, 2020. 1952 p.

LOPES JÚNIOR, Aury. **Direito processual penal**. 19. Ed. São Paulo: Saraiva, 2022. E-book.

MICHAUD, D.J. **Adventures in computer science**. SANS Institute, 2001.

NATIONAL INSTITUTE OF JUSTICE (NIJ). **Electronic Crime Scene Investigations: A Guide for First Responders**. 2nd Edition. NCJ 219941. Washington, DC. 2008.

NATIONAL INSTITUTE OF JUSTICE (NIJ). **Investigative uses of technology: devices, tools, and techniques**. NIJ Special Report NCJ213030. Washington, DC. 2007