Função '*hash*' e a integridade da prova digital

'Hash' *Function and Digital Evidence Integrity*

Yuri Fisberg[1]

Universidade de São Paulo – São Paulo, SP, Brasil

yfisberg@usp.br

http://lattes.cnpq.br/4348179257348250

https://orcid.org/0009-0008-1220-6846

Resumo: O artigo aborda a função *'hash'* como ferramenta para garantir a integridade de dados digitais, examinando seus fundamentos, limitações e aplicação no contexto da cadeia de custódia de provas digitais. A despeito das previsões do Código de Processo Penal, as constantes inovações tecnológicas implicam desafios por sua natureza imaterial e volátil, que também tornam difícil padronizar e regulamentar os processos de coleta e preservação. A partir da leitura interdisciplinar da técnica computacional, dos fundamentos matemáticos e criptográficos com o exame jurisprudencial dos acórdãos do STJ que abordam a temática, a função '*hash*' é apresentada como (mais) uma técnica eficiente para verificar a integridade de dados digitais; mas não infalível, sujeita a limitações devido ao avanço das tecnologias de criptografia e ao risco de obsolescência de certos protocolos. O artigo demonstra inconsistências e divergências em precedentes sobre o tema, destacando a necessidade de equilíbrio entre o uso dessas ferramentas e a vigilância crítica sobre sua aplicação no contexto judicial. Conclui-se que, apesar das limitações, o código '*hash*' continua sendo uma ferramenta valiosa, mas deve ser aplicado com rigor técnico e conhecimento especializado, garantindo a confiabilidade da prova digital sem prejudicar o devido processo legal.

Palavras-chave: cadeia de custódia; *hash*; integridade digital; processo penal; forense.

[1] Doutorando da Faculdade de Direito da Universidade de São Paulo (Departamento de Processo – Penal). Mestre em Direito pela Universidade de São Paulo. Especialista pela Escola Paulista da Magistratura. Promotor de Justiça do Ministério Público do Estado de São Paulo.

Abstract: *The article addresses 'hash' function as a tool to ensure digital data integrity, examining its foundations, limitations and application in the context of the chain of custody for digital evidence. Despite the provisions of the Code of Criminal Procedure, constant technological innovations present challenges due to the intangible and volatile nature of digital evidence, which also complicates the standardization and regulation of collection and preservation processes. From an interdisciplinary perspective, the 'hash' function could be used as an effective technique for verifying the integrity of digital data, but it is not infallible, subject to limitations due to advancements in encryption technology and the risk of obsolescence of certain protocols. The article demonstrates inconsistencies and divergences in precedents on the topic, highlighting the need for a balance between using these tools and maintaining critical oversight of their application in the judicial context. It concludes that, despite its limitations, the 'hash' code remains a valuable tool but must be applied with technical rigor and specialized knowledge, ensuring the reliability of digital evidence without compromising due process.*

Keywords: *chain of custody*; hash; *digital integrity*; *criminal procedure*; *forensic.*

1. INTRODUÇÃO

As últimas décadas refletem o movimento global de *virtualização*, "não apenas a informação e a comunicação, mas também os corpos"[2]. Exemplificando as conexões virtuais, no último Censo (2022) pouco mais de 60% dos domicílios brasileiros declararam estar conectados à rede de esgoto e saneamento[3], ao tempo que, levantamento de 2023, aponta93% da população nacional entre 16 e 63 anos como usuária do *WhatsApp*[4].

---

[2] LÉVY, Pierre. *O que é virtual?* Tradução Paulo Neves, 2ª Ed. São Paulo: Editora 34, 2011, p. 11.

[3] INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). *Censo 2022*, Panorama Brasil. Brasília: IBGE, 2022, disponível em: < https://censo2022.ibge.gov.br/panorama/indicadores.html?localidade=BR/>. Acesso em 18/11/2024.

[4] WE ARE SOCIAL & MELTWATER, *Digital 2023 Global Overview Report* (2023), disponível em <https://datareportal.com/reports/digital-2023-

E, além dos crimes cibernéticos[5], a "era da informação" alterou o fenômeno criminal. Embora "tão antigo quanto a própria humanidade", o "crime global" adquire outro patamar através da formação de "redes internacionais"[6]. A tecnologia trouxe "fatores novos" a diversos delitos, como ilustram a corrupção e a lavagem de capitais, impondo consequente "atualização" dos meios e métodos de investigação[7].

Em paralelo aos crimes *nato-digitais*, ou seja, praticados no ambiente eletrônico, a tecnologia pode envolver toda a gama de tipos e servir à acusação ou à defesa em praticamente qualquer processo. Conversas armazenadas, áudios trocados, imagens de câmeras de segurança, dados de localização, metadados de fotografias, histórico de pesquisas, postagens em redes sociais podem *representar* distintos elementos de convicção no raciocínio probatório.

Por suas características recorrentemente citadas na doutrina, imaterialidade, volatilidade, fragilidade e dispersão[8],, no entanto, a prova digital inspira especiais desafios às ciências jurídicas e forenses. As ciências aplicadas têm crescente relevância na admissibilidade e valoração das provas[9].

E, de forma recorrente, as decisões judiciais têm aludido ao código ou à função '*hash*'. Próprios da matemática inserida na ciência da

---

global-overview-report>. Acesso em 22/12/2024.

5 Sobre a relevância dos cibercrimes, confira-se a Convenção de Budapeste (Decreto n. 11.419, de 2023) e a recente Convenção da ONU sobre o tema (A/79/460).

6 CASTELLS, Manuel. *Fim de Milênio* – A Era da Informação – Economia, Sociedade e Cultura, v. 3. Trad. Klauss Brandini Gerhardt e Roneide Venancio Majer, 7ª ed. Rio de Janeiro: Paz e Terra, 2020, p. 373.

7 SILVA, Rafael Velasquez Saavedra da. Ferramentas Analíticas Aplicadas no Enfrentamento da Corrupção. In: JORGE, Higor Vinícius Nogueira (coord.). *Enfrentamento da Corrupção e Investigação Criminal Tecnológica* – Procedimentos, fontes abertas, estudos de casos e direito anticorrupção. Salvador: JusPodivm, 2020, p. 137/138.

8 MENDES NETO, José Guimarães. *Provas penais na era digital* – Desafios constitucionais e legais para recolha de dados à revelia do portador. Prefácio de Gilmar Mendes. São Paulo: Marcial Pons, 2024, p. 220-239.

9 ALCOCEBA GiL, Juan Manuel. Los estándares de cientificidad como criterio de admisibilidad de la prueba científica. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 4, n. 1, p. 215-242, jan./abr. 2018.

computação e da criptografia, os algoritmos de função '*hash*' têm adquirido protagonismo no campo da cadeia de custódia, notadamente após a Lei n. 13.964, de 2019. Contudo, dissonantes decisões e, principalmente, o vetor técnico olvidado sobre a temática inspiram especial apreensão.

Antes de *idolatrar* o 'código *hash*', é preciso compreendê-lo. O artigo pretende esclarecer o que é e para que serve a função '*hash*', em uma análise interdisciplinar que combina: a análise técnica-computacional dos fundamentos matemáticos e criptográficos da função '*hash*'; e o exame jurisprudencial dos acórdãos do Superior Tribunal de Justiça (instância uniformizadora da interpretação da legislação federal) que abordam a temática, identificando padrões decisórios e inconsistências.

2. '*HASH*'

O entendimento dos limites da tecnologia impõe estudo estranho ao direito. Inicialmente, vale também a referência à etimologia da expressão – sem tradução usual no país, o que, desde logo, ilustra algumas das preocupações doravante analisadas.

Com primeiro registro no dicionário *Oxford* de 1653, a expressão inglesa '*hash*' deriva da palavra francesa '*hacher*' – picar, cortar, em tradução livre. E a frequência na língua inglesa denota a evolução do emprego pouco recorrente em sua acepção remota da culinária dos anos 1600 até o incremento com o significado próprio do vocabulário da informática e criptografia, já na segunda metade do século XX[10].

No Brasil, a expressão é consagrada em língua estrangeira[11]. O Tribunal Superior Eleitoral utiliza a tradução "resumos digitais", mas

---

[10] OXFORD ENGLISH DICTIONARY, s.*v. Hash (n. 1) e (n. 3)*. Disponível em: <https://doi.org/10.1093/OED/6068424098>. Acesso 15/11/2024.

[11] A *função* '*hash*' ou o *código* '*hash*' já foram citados no Provimento n° 100, de 2020, do Conselho Nacional de Justiça (art. 22, §3º) – substituído pelo Provimento n° 149, de 2023, que também cita a tecnologia para a "autenticação notarial". No âmbito do registro de patentes, o Manual do Usuário do INPI também recomenda a "transformação, em resumo digital *hash*, dos trechos do programa de computador e de outros dados que considerar suficientes e relevantes para identificá-lo" (INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL. *Manual do Usuário para registro eletrônico de Programas de*

sempre acompanhada da referência *'hashes'*[12]. Na jurisprudência, os tribunais pátrios endossam de forma recorrente o verbete em inglês[13] próprio de *vocabulário técnico* – o que justifica, desde logo, a *especificidade* e *técnica* com que deve ser tratado o tema.

Mas, afinal, o que significa *'hash'*?

2.1 O QUE É '*HASH*'?

"Funções *hash* são algoritmos matemáticos determinísticos que mapeiam dados de comprimento aleatório em saída de tamanho fixo em base hexadecimal, dispersando os bits de entrada de forma não correlacionada às mudanças"[14]. Em termos mais simples, é um cálculo matemático que reduz um montante de dados em uma sequência alfanumérica *fixa* – um *corte* de *bits* e o processamento em um padrão, segundo um protocolo pré-determinado.

Computador. Diretoria de Patentes, Programas de Computador e Topografias de Circuitos Integrados. Helmar Alvares, Antônio Carlos Coelho e Matheus Souza Pinto Engel. Rio de Janeiro: INPI, 2022, p. 10).

[12] Citando: "O Resumo digital corresponde a um código único, tal como um identificador que pode ser recalculado por qualquer pessoa. É como uma forma de calcular uma impressão digital de um arquivo, com uma fórmula de cálculo conhecida por todos. O algoritmo, ou fórmula de cálculo, para um resumo digital se chama *algoritmo de hash*. O *hash* é, então, uma técnica criptográfica que gera uma identificação única para um arquivo digital. Assim, qualquer alteração no arquivo para o qual um *hash* foi calculado, geraria um resumo digital completamente diferente e a alteração seria facilmente detectada, mesmo se fosse apenas uma única letra" (TRIBUNAL SUPERIOR ELEITORAL. *Glossário de TI*. Brasília: TSE, 2024, disponível em: <https://www.tse.jus.br/comunicacao/glossario-de-ti>. Acesso em 24/12/2024).

[13] Cf. STF, HC 248.587, Min. Alexandre de Moraes, DJ 12/11/2024; STJ, RHC n. 205.088, Ministro Ribeiro Dantas, DJe de 20/12/2024; TJAC, AP 0001573-66.2023.8.01.0001, Rel. Des. Francisco Djalma, DJe 17/12/2024; TJRS, AP 50030072620238210008, Rel. Des. Orlando Faccini Neto, DJe 28/11/2024; TJMA, AP 0020540-57.2016.8.10.0001, Rel. Des. Jose Luiz Oliveira de Almeida, DJe 11/10/2023. TJSP, HC 2331340-15.2024.8.26.0000, Rel. Des. Renata William Rached Catelli, DJe 19/12/2024.

[14] SILVA, Johan Matos Coelho da; SILVA, Philipe Matos Coelho da. *Técnicas de detecção e classificação de malwares baseada na visualização de binários*. Monografia. Universidade de Brasília, Engenharia de Redes de Comunicação, 2018, p. 20.

O progresso da *internet*, a troca de informações e o comércio eletrônico basearam-se (e dependem continuamente) de *novos* instrumentos aptos a conferir integridade e confiabilidade. A tecnologia permite o suplantar da "arte antiga" para introduzir a criptografia na ciência que alterou substancialmente o panorama das relações à distância e das telecomunicações[15] e, nesse contexto, as diversas *funções 'hash'* surgem no campo da programação e da criptografia como mecanismo de *autenticação* e conferência de *integridade* de um pacote de dados.

As criptografias antigas tinham o êxito baseado no "segredo de todo o processo de encriptação". O advento dos computadores, porém, substitui o sigilo por protocolos que transitam as informações em *canal público*, com mecanismos de autenticação e encriptação também públicos e que servem à certificação da comunicação e da identidade dos interlocutores[16].

A *função 'hash'* nada mais é que um algoritmo matemático que transforma uma entrada de dados (*'input'*) em uma expressão alfanumérica de *formato pré-determinado* (*'output'*) de complexa reversão ou repetição. Logo, a ferramenta surge no âmbito da programação e da criptografia por gerar um *'output'* pode transitar em redes abertas, uma expressão "extremamente difícil de recriar os dados originais (*'input'*) a partir do valor do *hash* sozinho" – característica chamada de "resistência à colisão"[17].

---

[15] DIFFIE, Whitfideld; HELLMAN, Martin E. "New Directions in Cryptography" in *IEEE Transactions on Information Theory*, Vol. IT22, n° 6, pp. 644-654, novembro de 1976, p. 644.

[16] Idem, p. 654.

[17] "The essence of the blockchain is informational before being economic or monetary, conducive to many emerging and increasingly popular token-free blockchains. It relies extensively on *hashes* and *hash* functions. A *hash* (output) is the result of a transformation of the original information (input). A *hash* function is a mathematical algorithm that takes an input and transforms it into an output. A cryptographic *hash* function is characterized by its extreme difficulty to revert, in other words, to recreate the input data from its *hash* value alone. This is called the collision resistance" (PILKINGTON, Marc. "Blockchain Technology: Principles and Applications" in OLLEROS, F. Xavier; ZHEGU, Majlinda. *Research Handbook on Digital Transformations*. Northampton (MA-EUA): Edward Elgar, 2016, disponível em: <https://ssrn.com/abstract=2662660>. Acesso em 23/12/2024.

Em suma, são cálculos que partem da premissa de que "o trabalho de desfazer o processo" de encriptação tome "tanto tempo que ninguém conseguisse pô-lo em prática". É um problema matemático "fácil de fazer e difícil de desfazer"[18].

E, surgida nas tecnologias de programação, plurais em protocolos de *'blockchain'* e criptomoedas, a *função 'hash'* também serve de autenticação, na medida em que *mínima alteração* ou *diferença* nos dados de entrada (*'input'*) reproduzem uma expressão totalmente distinta. "Uma pequena mudança na entrada, seja um simples caractere em uma frase inteira, ou um pixel em uma foto, acarreta uma saída completamente diferente, sendo essa característica conhecida como Efeito Avalanche"[19].

Exemplificando, o parágrafo antecedente gera um *'hash'* no protocolo MD5 sem o ponto final (9b60590724ef2a7f072ce60f53fb106b) totalmente diverso em relação àquela mesma frase com a mínima inclusão da pontuação (0147e0dc7bee5555e05eb9005eb0511a).

Por isso, afirma-se que o *'hash'* pode traduzir a *impressão digital* (*'fingerprint'*) de um arquivo ou conjunto de dados.

2.2 Protocolos

A *função 'hash'* serve, por exemplo, à autenticação na transferência de dados pela *internet*, preservação de um código fonte na programação ou assinatura digital. Para tanto, são *dezenas* de algoritmos com complexidade matemática e computacional diversas que, consequentemente, podem produzir *'hashes'* diferentes, de reprodução, replicação e integridade mais ou menos confiável, a depender da tecnologia empregada[20].

---

[18] LIGUORI, Carlos. *Direito e Criptografia*: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia 1ª Ed. São Paulo: SaraivaJur, 2022, p. 35.

[19] SILVA, Johan Matos Coelho da; SILVA, Philipe Matos Coelho da. *Técnicas de detecção e classificação de malwares baseada na visualização de binários*. Monografia – Universidade de Brasília, Engenharia de Redes de Comunicação, 2018, p. 21.

[20] Ilustrando, a palavra "criptografia" pode ser expressa com os '*hashes*' em protocolo CRC16 de apenas quatro caracteres (382a) ou outros mais extensos e, por consequência, mais seguros e confiáveis, como o

A distinção está associada à evolução da tecnologia. Afirmar a "difícil" reversão de um cálculo matemático depende do contexto computacional e tecnológico; em geral, os protocolos de criptografia e *funções 'hash'* estão baseados em cálculos de grandeza de complexa fatoração, de modo que identificar a ordem dos *bits* de entrada (*'input'*) poderia demorar "zilhões de anos"[21].

Logo, os protocolos são *substituídos*, incrementados e alterados ao longo do tempo, com a evolução do processamento das máquinas e documentada fragilidade de modelos anteriores.

Criados na década de 1990, os algoritmos MD4 e MD5 geram *'hashes'* de 128 *bits* – 32 caracteres hexadecimais[22] – inferiores aos atuais protocolos SHA (*'Secure Hash Algorithm'*). Os algoritmos SHA-1, SHA-256, SHA-224, SHA-384, SHA-512 têm a expressão numérica que representa a extensão dos bits do *'hash'* calculado, respectivamente 160, 256, 224, 384 e 512; portanto, com maior resistência a *colisões*[23].

Pouco tempo depois da criação, o MD4 e o MD5 foram *expostos* com a demonstração matemática de *colisões*, isto é, de *'hashes'* idênticos para dados de entrada inicial *diferentes*[24]. No mesmo sentido, o SHA-0, de 1993, foi considerado obsoleto em 1996, quando substituído pelo SHA-1,

---

MD5 (97c6105c1d97d600ec16ab4abace6d4c); o protocolo *Whirlpool* de domínio público (dd26a2ca3ee84077c572fcea02900046d6c619cabe6de694a2deac01aad4b9d23da3726b412a6212385d430165b5215c769c5e61e7d9d51304904bcf670ff7e0); o protocolo SHA512 (e3b39ab14385b0f4faf1ff5fd634f7fb204e9e6a2ccc35e90c2a9fb863763f640243ef582f994757b1e552cff6a4bae5c9b100093c6a5160f4e22c3b4236210b).

21 COUTINHO, Severino. *Criptografia*. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada, 2016, p. 10.

22 RIVEST, Ronald Linn. The MD4 Message Digest Algorithm. *RFC* 1320, abril de 1992. Boston: MIT and RSA Data Security Inc., 1992.

23 TILBORG, Henk C.A. van; JAJODIA, Sushil (ed.). *Encyclopedia of Cryptography and Security*, 2a ed. New York: Springer, 2014, p. 1192

24 WANG, Xiaoyun; YU, Hongbo. "Collisions for *hash* functions MD4, MD5, HAVAL-128 and RIPEMD" in *Proceedings of the Annual International Cryptology Conference* (CRYPTO), 2005. p. 123–138. Disponível em: <https://www.semanticscholar.org>. Acesso em 22 dez. 2024; e ZAIKIN, Oleg. Inverting cryptographic *hash* functions via cube-and-conquer. *Journal of Artificial Intelligence Research,* 81, 2024, pp. 359-399. Disponível em: <https://dl.acm.org/doi/pdf/10.1613/jair.1.15244>. Acesso em 22 dez. 2024.

justamente porque demonstrada violação no teste de "colisão" – ou seja, de possível *repetição* a partir de entradas diversas[25].

E, embora *fraco* contra teses de *colisão*, o protocolo MD5 de *função 'hash'* segue com uso disseminado em testes de *integridade* de arquivos. Isto porque, a extensão e complexidade de um algoritmo repercutem em outros aspectos distintos da segurança, igualmente importantes na adoção e uso de uma tecnologia – afinal, o *tempo* de cálculo e conferência é proporcional à complexidade do algoritmo[26].

Hoje, considerado mais "seguro", o protocolo SHA-512 pode demorar o *dobro* ou *triplo* do tempo de processamento em comparação ao SHA-256 a depender do volume de dados e natureza dos arquivos do *'input'*[27]. E, por isso, as normas internacionais de padronização de segurança da informação não elegem um único protocolo[28]; ao contrário, até o padrão MD5 considerado *obsoleto* para a "autenticação" segue útil como mecanismo de verificação da integridade e de eventual manipulação "não intencional" de dados[29].

---

[25] BIHAM, E., CHEN, R., JOUX, A. et. al. "Collisions of SHA-0 and Reduced SHA-1" in CRAMER, R. *Advances in Cryptology* – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Berlin: Springer, 2005, p. 44, disponível em: <https://doi.org/10.1007/11426639_3>. Acesso em 18/12/2024.

[26] ARSLAN, Engin; ALHUSSEN Ahmed. "Fast integrity verification for high-speed file transfers" in *arXiv preprint arXiv:1811.01161*, 2018. Disponível em: <https://arxiv.org/pdf/1811.01161>. Acesso em 17/11/2024.

[27] HASHIM, Hasan; ALZIGHAIBI, Ahmad Reda; ELESSAWY, Amaal Farag [et. al.]. Securing Financial Transactions with a Robust Algorithm: Preventing Double-Spending Attacks. *Computers* 12, n. 9: 171, 2023.

[28] As funções *'hash'* são documentadas em norma internacional como a padronização ISO/IEC 10118-3:2018 – disponível em: <https://www.iso.org/standard/67116.html>.

[29] KAUFMANN, Alex; GARTMON, Emelie. Comparative Analysis of Different Cryptographic *Hash* Functions, Degree Project. *Technology*, KTH Royal Institute of Technology, 58p, Stockholm, 2024. Disponível em: <https://kth.diva-portal.org/smash/get/diva2:1885074/FULLTEXT01.pdf>. Acesso em 23/12/2024.

2.3 O QUE NÃO É '*HASH*'?

Em contraposição, os conceitos trazidos permitem expor as limitações ínsitas ao *'hash'* – especificamente para o que ele *não* serve.

Nos diversos modelos, a *função 'hash'* é talvez o "mais versátil algoritmo da criptografia", disseminado em aplicações de segurança e inúmeros protocolos de programação e de internet[30] - o que, todavia, não significa a intangibilidade. É necessário compreender a *finalidade* da tecnologia, para aferir sua utilidade e reconhecer os *limites* da função.

A versatilidade do algoritmo permite o cálculo *'hash'* de basicamente *qualquer* pacote ou volume de dados. É possível gerar um código *'hash'* de um texto, uma fotografia, um vídeo ou centenas/milhares de arquivos. Pode-se reduzir a um *'hash'* a íntegra da cópia de um *hard--drive* de computador ou o conjunto de imagens (extração) de diversos computadores.

A referência do *'hash'* como ferramenta de autenticação está, em verdade, associada à *autenticidade* de um dado – ou seja, se determinado arquivo ou pacote de dados não foi manipulado, falsificado ou forjado de qualquer modo[31]. O *'hash'* serve de parâmetro para confirmar a autenticidade de um arquivo transferido, permitindo a *comparação* entre a fonte e a origem, mas, por si, não significa a identidade ou autenticação do conteúdo ali existente.

O *'hash'* de uma imagem ou vídeo atesta apenas a integridade do pacote de dados (bytes) ali reunidos em comparação ao estado que fornecido/disponibilizado na origem. Sozinho, o *'hash'* não significa a *veracidade* ou *fonte* da imagem/mídia. Ainda que a tecnologia permita o rastreio da cadeia de autoria – como ocorre nos chamados NFTs[32] -,

---

[30] STALLINGS, William. *Cryptography and Network Security* – principles and practice, 7th ed., global edition. London: Pearson, 2017, p. 341.

[31] MENEZES, Alfred J.; OORSCHOT, Paul C. van; VANSTONE, Scott A. *Handbook of Applied Cryptography*, 2nd ed. Boca Raton (FL-EUA): CRC Press, 1996, p. 322-327.

[32] CANTALI, Fernanda Borghetti. *A Tokenização da Arte Visual e o Direito Autoral*: o Copyright by Design e a definição das premissas mínimas de governança para viabilizar o NFT – Non Fungible Token como instrumento de negociação de obras de arte. Brasil: Editora Dialética, 2024.

o *'hash'* nada mais é que um resumo hexadecimal do arquivo, sem valor quanto à autenticidade de seu conteúdo[33].

Ilustrando em temática recorrente à prova penal, é possível gerar *'hash'* de uma fotografia, de uma imagem da tela de um computador ou da *captura* de um celular (*'print'*) – o que não significa nada em relação ao conteúdo destes arquivos. O *'hash'* não serve para distinguir, por exemplo, se a uma fotografia foi *criada* por inteligência artificial. Igualmente, o *código 'hash'* e imagem de suposta conversa em aplicativo de mensagens (*WhatsApp*) não significa a integridade da conversa – possível, do mesmo modo, que o *'chat'* tenha sido criado em emulador.

Se, por sua natureza determinística, a mínima alteração da fonte implica na alteração do *'hash'*, alguns arquivos efetivamente *jamais* poderão ter o código replicado – isto é, conferido.

Arquivos temporários, bases de dados mutáveis ou pacotes com *'timestamp'* não replicarão um mesmo *código 'hash'* – ainda que sem *manipulação* humana ou alteração do conteúdo. A dificuldade do cálculo *'hash'* em *logs* de acesso a um sistema ou de páginas da *internet* e URLs comuns são exemplos do obstáculo ínsito à natureza tecnologia[34].

Exemplificando, uma página que traz notícia escolhida de forma aleatória da *internet*, publicada em portal de notícias *on-line* da Folha de São Paulo, reflete um arquivo .html com textos dinâmicos, possibilidade de atualização pelo provedor, *banners* de publicidade personalizados, rol de comentários e notícias relacionadas cambiáveis[35]. *Qualquer* alteração, mesmo que íntegro o texto da notícia, não reproduziria um mesmo código *'hash'*.

---

[33] Protocolos "mistos" ou combinados de *'hash'* com outros modelos de criptografia permitem a vinculação à identidade, como nas hipóteses de assinaturas digitais (MISAGHI, Mehran. *Um Ambiente Criptográfico Baseado na Identidade*. Tese – Universidade de São Paulo (Escola Politécnica), 2008).

[34] ATURBAN, Mohamed; NELSON, Michael L.; WEIGLE, Michele C. Difficulties of Timestamping Archived Web Pages. *arXiv preprint arXiv:1712.03140*, 2017. Disponível em: <https://arxiv.org/abs/1712.03140>. Acesso em 23 dez. 2024.

[35] Exemplificando: https://www1.folha.uol.com.br/tec/2024/12/o-chip-quantico-do-google-que-resolve-em-5-minutos-problema-que-levaria-10-septilhoes-de-anos.shtml

Veja-se, é possível extrair ou imprimir o conteúdo em arquivo de texto (.txt ou .pdf) ou imagem (.jpeg) e, sobre este arquivo, calcular um código *'hash'* repetível. A cada extração ou impressão, no entanto, o *'hash'* será distinto e a função provará, tão-somente, a integridade *daquele* arquivo outrora impresso em determinada circunstância.

Repetindo a hipótese do *'print'* de conversas armazenadas em um celular, o cálculo de *'hash'* da mera captura (que nada se correlaciona com a fonte ou conteúdo) é pouco relevante para a fiabilidade da prova. O cálculo apenas repercutirá a preservação da imagem, do conjunto de *pixels* ali reunido em determinado momento, sem aptidão de reunir, por exemplo, os dados e metadados que permitam maior análise da conversa, dos interlocutores ou de seu conteúdo.

3. '*HASH*' E A CADEIA DE CUSTÓDIA

Introduzida a *função 'hash'*, deve-se reconhecer a crescente referência e utilidade da ferramenta à cadeia de custódia das provas digitais.

A Lei n° 13.964, de 2019, introduziu no Código de Processo, a preocupação com a cadeia de custódia há muito citada na doutrina como pressuposto de um "rigoroso sistema de controles epistêmicos"[36] exigível do processo penal.

Na doutrina, uníssono o destaque da relevância do tema para o devido processo legal e o contraditório. "A manutenção da cadeia de custódia é de suma importância, pois é ela quem garante ao réu que a prova trazida pela acusação é a mesma que foi obtida na investigação ("mesmidade"), em observância aos procedimentos legais e sem alterações ("desconfiança")"[37].

Ainda que os pormenores do tratamento da cadeia de custódia dos artigos 158-A a 158-F, do Código de Processo Penal, não versem

---

[36] PRADO, Geraldo. *Prova Penal e sistema de controles epistêmicos*, 1ª ed. São Paulo: Marcial Pons, 2014, p. 43

[37] SOUZA, Lia Andrade de; VASCONCELLOS, Vinicius Gomes de. A cadeia de custódia da prova obtida por meio de interceptações telefônicas e telemáticas: meios de proteção e consequências da violação. *Revista da Faculdade de Direito UFPR, [S. l.]*, v. 65, n. 2, p. 31–48, 2020..

"especificamente" sobre os vestígios digitais, tais regras são "também observáveis quanto ao dado cibernético"[38]. O problema é que, "no mundo digital, a distinção do original e da cópia há muito perdeu qualquer pertinência. O ciberespaço está misturando as noções de unidade, de identidade e de localização"[39].

A superação global do modelo, outrora baseado em evidências físicas e provas testemunhais, para um processo lastreado em vestígios digitais deve "inspirar" um novo processo criminal[40]. Por sua natureza, as evidências digitais são marcadas pela *dispersão,* com transcendência das fronteiras nacionais e distanciamento entre servidores e computadores pessoais[41]. Igualmente, a *desmaterialização* acresce riscos de *volatilidade* à prova, com "alto grau de vulnerabilidade a erros"[42].

Na Convenção de Budapeste, internalizada pelo Decreto n. 11.491, de 2023, o Brasil se compromete a adotar "medidas legislativas e outras providências necessárias" para "promover investigações ou processos criminais" em crimes cibernéticos – inclusive na "coleta de provas eletrônicas da prática de um crime"[43].

Assim, na consecução das normas, seria *desejável* a eleição de uma "técnica específica" para o tratamento dos vestígios digitais.

Contudo, tal solução é "inviável", já que "ainda não há meios e técnicas uniformemente aceitos e, de outro, que tem havido rapidíssima mutação e evolução das técnicas computacionais"[44]. Padrões

---

[38] ESPIÑEIRA, Bruno; et al. *A prova e o processo penal constitucionalizado:* estudos em homenagem ao ministro Sebastião Reis. Belo Horizonte: Editora D´Placido, 2021. *E-book.* p.67.

[39] LÉVY, Pierre. *O que é virtual?* Ob. Cit., p. 48.

[40] KERR, Orin S. "Digital Evidence and the New Criminal Procedure" in 105 *Columbia Law Review*, pp. 279-318, 2005. Disponível em: <https://ssrn.com/abstract=594101>. Acesso em 25/12/2024.

[41] DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di Diritto Processuale*, Padova, s.2 a.66 n.2 (marzo-aprile 2011), p.283-298.

[42] BADARÓ, Gustavo. Os standards metodológicos de produção da prova na prova digital e a importância da cadeia de custódia. *Revista IBCCRIM*, São Paulo, v. 343, ano 29, p. 7-9, jun./2021, p. 8.

[43] Decreto 11.491/2023, artigo 14. 1 e 2.c.

[44] BADARÓ. Os standards metodológicos... Ob. cit., p. 7.

"excessivamente específicos" seriam *inúteis* a médio e longo prazo[45], com formalização que pode se tornar "obsoleta"[46]. Embora se aponte legislações estrangeiras que também disciplinam de forma "detalhada" a cadeia de custódia na lei[47], o que se vê usualmente é a remissão a outras normas infralegais que efetivamente regulamentam a matéria em razão da preocupação com a evolução tecnológica. Exemplifica, aqui, o Código de Processo Penal da Colômbia[48].

Em verdade, até as normativas *infralegais* sobre evidências digitais repetem o caráter amplo, definindo princípios gerais não necessariamente associadas a uma ou outra tecnologia.

Ilustrando, no plano internacional a *Internet Engineering Task Force (IETF)*, responsável exatamente pela organização de padrões de funcionamento da rede mundial de computadores, emitiu em 2002 a RFC

---

45 "Tale canone è, forse, in grado di cogliere quella che è la particolarità maggiore delle evidenze di carattere informatico, ossia la loro costante e rapida evoluzione. Sotto questo profilo il compito affidato al legislatore non appare affatto leggero. Un intervento eccessivamente specifico rischierebbe di essere inutile in un'ottica di medio-lungo periodo' (MURGIA, Severino. *Prova Informatica e Processo Penale*. Tese – Università Degli Studi di Pavia, Pavia, 2017, p. 235).

46 DANIELE, Marcello. Ob. Cit., p. 293.

47 BARTOLI, Laura. La catena di custodia del materiale informatico: soluzioni a confronto, 2016. *Anales de la Facultad de Derecho*, 33, Bologna, 2016, p. 147.

48 O artigo 254 do Código de Procedimento Colombiano prevê que o Ministério Público regulamentará o sistema de cadeia de custódia "de acordo com os avanços científicos, técnicos e artísticos" – o que está, efetivamente, regulado pela Resolução n. 0-6394/2004. "ARTÍCULO 254. Aplicación. Con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos. La cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física, y finaliza por orden de autoridad competente. Parágrafo. El Fiscal General de la Nación reglamentará lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, de acuerdo con los avances científicos, técnicos y artísticos" – disponível em: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787>.

3227[49] que fixa *Diretrizes para Coleta e Armazenamento de Evidências*[50]. Sem aderir a qualquer ferramenta ou protocolo específico, o documento fixa princípios para preservação da coleta de evidências, documentação minuciosa da cadeia de custódia e de todos os procedimentos.

A preservar a integridade dos registros, o RFC 3227 recomenda a *cópia em nível de 'bits'* (*'bit-level copy'*) referindo que a análise forense "quase certamente" altera a evidência, que deve ser preservada em cópia[51]. Descreve, então, de forma exemplificativa algumas "ferramentas" necessárias, como programas para a cópia fiel da mídia e outros aptos a gerar *'checksums'* e assinaturas[52].

De modo semelhante, a *National Institute of Standards and Technology*, agência governamental norte-americana, tem *Guia para a Integração de Técnicas Forenses* (SP 800-86)[53].

No capítulo que retrata as técnicas de cópia de arquivos de mídia, contempla genericamente hipóteses de *'backup lógico'* ou de extração de imagem *'bit a bit'* que produzem "cópia exata" do repositório – exemplificando que "numerosos *hardwares* e *softwares* podem realizar a tarefa da imagem *bit a bit* ou o *'backup lógico'*", alguns, inclusive com ferramentas nativas de *função 'hash'*, com a ressalva de que a exemplificação de

---

[49] Disponível em: https://datatracker.ietf.org/doc/rfc3227/

[50] INTERNET ENGINEERING TASK FORCE (IETF). *Guidelines for Evidence Collection And Archiving,* Network Working Group, D. Brezinski, Best Current Practice, fev. 2002. Disponível em: <https://www.rfc-editor.org/rfc/pdfrfc/rfc3227.txt.pdf>. Acesso em 03/01/2025.

[51] "2. (...) - You should make a bit-level copy of the system's media. If you wish to do forensics analysis you should make a bit-level copy of your evidence copy for that purpose, as your analysis will almost certainly alter file access times. Avoid doing forensics on the evidence copy".

[52] "5. (...) Your set of tools should include the following: (...) - a program for doing bit-to-bit copies (e.g., 'dd', 'SafeBack'). - programs for generating checksums and signatures (e.g., 'sha1sum', a checksum-enabled 'dd', 'SafeBack', 'pgp')".

[53] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Special Publication (SP) 800-86* Guide to Integrating Forensic Techniques into Incident Response, Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, Technology Administration. Gaithersburg: U.S. Department of Commerce, 2006.

determinada aplicação não significa qualquer "endosso" ao produto[54] No Brasil, a RFC 3227 é referenciada expressamente como fonte da Norma Brasileira ABNT ISO/IEC 27037:2013[55].

Sem escopo de substituir "exigências legais de qualquer jurisdição", o padrão ABNT prevê "diretriz prática" para a investigações "envolvendo potenciais evidências digitais" no sentido de "manter a integridade da evidência". Fixa, expressamente, a prioridade de "minimizar o risco de a potencial evidência digital ser espoliada e maximizar o seu valor probatório"[56].

Ainda no glossário, a norma de padronização prevê como "função de verificação" aquela que é utilizada "verificar [se] dois conjuntos de dados são idênticos". Importante nota com ressalva sobre o tópico: "funções de verificação são comumente implementadas utilizando funções '*hash*' como MD5, SHA1 etc., mas outros métodos podem ser utilizados"[57].

Cumprindo sua natureza, a norma da ABNT serve de lastro a outras tantas regulamentações e diretrizes que servem à preservação de vestígios e posterior instrução criminal. Ainda que não prevejam expressamente a *função 'hash'* ou algum protocolo ou método análogo, mesmo que evidentes os limites da tecnologia, diversos órgãos têm referendado a técnica da preservação e integridade dos vestígios digitais[58].

---

[54] "Numerous hardware and software tools can perform bit stream imaging and logical backups. Hardware tools are generally portable, provide bit-by-bit images, connect directly to the drive or computer to be imaged, and have built-in *hash* functions. (...) Examples of hardware-based disk imaging tools are Image MASSterís SOLO Forensics (http://www.ics-iq.com/) and Logicubeís Solitaire (http://www.logicube.com/). Additional products are referenced in Web sites listed in Appendix F, including The Ultimate Collection of Forensics Software (TUCOFS) (http://www.tucofs.com/tucofs/tucofs.asp?mode=filelist&catid=10&oskey=12). The applications referenced throughout this publication are by no means a complete list of applications to use for forensic purposes, nor does this publication imply any endorsement of certain products" (Idem, p. 4-6).

[55] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27037:2013*. Rio de Janeiro: ABNT, 2013.

[56] Idem, p. 6.

[57] Item 3.25, idem, p. 4.

[58] O Gabinete de Segurança Institucional da Presidência da República tem norma técnica sobre "incidentes de segurança em redes" com a imposição da

De forma uníssona, a melhor prática forense recomenda que a evidência digital armazenada seja extraída (espelhamento *'bit a bit'*) antes da análise, o que, em tese, permite a conferência da integridade do vestígio digital. Para esta situação, o '*hash*' – ou os *'hashes'* se combinados mais protocolos – serve justamente a demonstrar a fiabilidade do pacote extraído da fonte.

O cálculo *'hash'* sobre determinado pacote de dados deve servir de *presumida satisfação* da exigência exposta no artigo 158-B, do Código de Processo Penal. É o tratamento esperado na utilização do vestígio, mas, nem de longe, exclusivo, exaustivo ou peremptório sobre a (in) admissibilidade ou a valoração da prova digital.

Seja pela insegurança de determinado protocolo e das possíveis *colisões* propositais; pela obsolescência tecnológica dos cálculos *'hash'* ante a evolução do processamento computacional; seja pelas limitações ínsitas da tecnologia e do seu caráter determinístico, não útil a todo e qualquer arquivo, tal presunção é *relativa*. Satisfaz o *ônus* do Estado sobre a cadeia de custódia do vestígio; no entanto, não exclui *outros* métodos de preservação da evidência, tampouco torna absoluto aquilo que se quer provar.

O *'hash'* é uma ferramenta útil, mas não resolve todos os desafios relacionados aos vestígios digitais. E, loquazes do risco da *idolatria* ao *'hash'*, as divergências sobre o tema no Superior Tribunal de Justiça expõem a dificuldade nas tentativas de se avançar na regulamentação da cadeia de custódia em meio a influxos voluntaristas, consequencialismo e carente coerência técnica ou forense.

---

documentação rigorosa e preservação dos arquivos com o cálculo dos "resumos criptográficos". No Glossário, a norma define Resumo Criptográfico: "4.18. Resumo Criptográfico: é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho desta, gera um resultado único e de tamanho fixo, também chamado de '*hash*'" (PRESIDÊNCIA DA REPÚBLICA. *Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes*, Gabinete de Segurança Institucional, 21/IN01/DSIC/GSIPR, 08 de outubro de 2014. Disponível em: <https://www.gov.br/gsi/pt-br/ssic/legislacao/NC21.pdf>).

3.1 '*Hash*' na Jurisprudência do STJ

Antes da análise dos precedentes de provas digitais e '*hash*' no âmbito do STJ, registra-se ressalva sobre o recorte de processos criminais sob pesquisa.

Dados do Anuário Brasileiro de Segurança Pública atestam a inversão nas estatísticas de crimes de roubos e estelionatos entre 2018 e 2023. Observando a "tendência mundial", a "transformação digital" repercute no número "crescente de estelionatos e golpes virtuais", em virtude da "migração mais intensa de esferas da vida para o ambiente cibernético"[59].

Contudo, o panorama das ocorrências policiais registradas ainda é bastante diverso daquele das investigações e ações penais – associadas à lógica do auto de prisão em flagrante e dos crimes *analógicos*. A maioria dos processos ainda decorre de prisões em flagrante, oriunda de delegacias "não especializadas" e não depende de "diligências complementares" de investigação[60].

Por isso, afirmar a emergente preocupação da integridade das provas digitais na jurisprudência deve considerar o contexto estatístico.

O repositório do Superior Tribunal de Justiça apresenta algumas centenas de menções à expressão '*hash*'. Desde a primeira menção em decisão monocrática de 2012, há crescente referência; são 78 (setenta e oito) decisões criminais em 2024[61], mesmo período em que o Tribunal recebeu mais de 169 mil feitos criminais[62].

---

[59] ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2024. São Paulo: Fórum Brasileiro de Segurança Pública, ano 18, 2024, p. 99.

[60] COSTA, Arthur Trindade Maranhão; DE OLIVEIRA JUNIOR, Almir. "Novos padrões de investigação policial no Brasil" in *Sociedade e Estado*, v. 31, n. 1, p. 147–164, 2016. Disponível em: <https://periodicos.unb.br/index.php/sociedade/article/view/6083>. Acesso em 02/01/2025.

[61] Pesquisa livre no repositório de jurisprudência do STJ de decisões com o termo exato "*hash*" – sem limitação temporal, realizada na data de 03/07/2025. Tabela disponibilizada com a lista das decisões monocráticas e acórdãos encontrados – destacadas 13 (treze) decisões colegiadas, com duas de natureza cível; e 345 decisões monocráticas com a expressão, sendo 301 de natureza criminal e referência efetiva ao tema da função '*hash*'. Tabela de dados brutos depositada em SciELO Data: FISBERG, Yuri. Dataset de "Função '*hash*' e a integridade da prova digital". *SciELO Data*, V1, 2025. https://doi.org/10.48331/scielodata.T2RHA3

[62] SUPERIOR TRIBUNAL DE JUSTIÇA. *Boletim Estatístico – Novembro de 2024*. Brasília: STJ, 2024, p. 7. Disponível em: <https://www.stj.jus.br/

Ainda que o vestígio digital sirva à investigação e prova nos "crimes de rua", mesmo que possível tecnicamente calcular o código *'hash'* de qualquer conjunto de dados computacionais[63]; deve-se reconhecer que a contundência do debate surge em um nicho específico de provas. As provas digitais têm protagonismo em investigações diferenciadas, vez que é exigência da efetiva persecução da cibercriminalidade "novas modalidades de investigação"[64].

Eogan Casey rememora que tecnologia também favorece os "criminosos", igualmente "preocupados com as evidências digitais" a fim de "manipulá-las" para evitar a atuação dos órgãos de investigação. Consequentemente, a investigação digital tem demanda específica, com a expansão de técnicas e metodologias[65] - não raro, reúnem aqueles que estão acostumados com a "impunidade da macrodelinquência econômica"[66].

O recorte estatístico e a natureza dos processos sob análise, somados à exigência técnica própria da tecnologia em análise, impõem o alerta de que traçar critérios garantistas no tratamento da prova digital não pode reforçar um sistema penal "desigual" e "seletivo", sob pena de

---

docs_internet/processo/boletim/2024/Boletim202411.pdf>. Acesso em 03/01/2025.

63 A temática do *'hash'* surge, por exemplo, em processos de violência doméstica: no HC n. 916.564, em que a Ministra Daniela Teixeira rechaçou a tese do vício processual – "embora tenha argumentado com uma possível quebra da cadeia de custódia da prova, o recorrente não cuidou de demonstrar de que forma ela teria ocorrido, a tanto não se prestando a mera alegação de que o trabalho pericial foi realizado sem maiores cuidados" (STJ, HC n. 916.564, Ministra Daniela Teixeira, DJe de 28/05/2024); e, em precedente em sentido oposto, o Ministro Ribeiro Dantas, reconheceu a fragilidade dos *'prints'* que amparavam a condenação por ameaça – justamente porque ausente a extração observando-se a exigência do código *'hash'* (STJ, AREsp n. 2.682.451, Ministro Ribeiro Dantas, DJe de 03/12/2024).

64 KIST, Dário José. *Prova Digital no Processo Penal,* 2ª ed. rev., ampliada e atualizada. Leme: Mizuno, 2024, p. 103.

65 CASEY, Eoghan. *Digital Evidence and Computer Crime*: Forensic Science, Computers and the Internet. 3a ed. Burlington: Elsevier, 2011, p. 9.

66 GOMES, Luiz Flávio Gomes. A impunidade da macrodelinquência econômica desde a perspectiva criminológica da teoria da aprendizagem. Letras Jurídicas Revista Eletrónica de Derecho del Centro Universitario de la Ciénega, n. 12, 2011, p. 07. Disponível em: <http://letrasjuridicas.cuci.udg.mx/index.php/letrasjuridicas/article/view/128/126>. Acesso em 10 abr. 2019.

se chancelar judicialmente a reconhecida "vista grossa àqueles que detêm poder econômico e social"[67]. Nada perto de limitar garantias processuais ou as nivelar por baixo, deve-se reconhecer os riscos da imposição de determinados padrões de tratamento ou da sorte automática da prova digital pela falta ou falha do código '*hash*'.

Leitura dos precedentes da temática da cadeia de custódia, em específico aqueles que mencionam a expressão '*hash*' permite identificar divergências e contradições. As decisões repercutem soluções distintas a casos semelhantes e ausente maior reflexão técnico-científica. Na pesquisa singela do termo no repositório da jurisprudência até julho de 2025, são identificados treze decisões colegiadas do STJ que mencionam a expressão '*hash*'. Excluídos aqueles de natureza cível (dois julgados)[68], os demais se concentram na 5ª Turma, com um único acórdão da 6ª Turma e outro da Corte Especial.

Há um traço comum, também identificável em decisões monocráticas analisadas na sequência: a jurisprudência reconhece sanção processual[69] à absoluta falta de documentação da cadeia de custódia – independentemente da questão do '*hash*' ou outras técnicas de preservação da integridade dos dados, há padrões *mínimos* que amparam o juízo de admissibilidade e ensejam o reconhecimento de nulidade da prova.

Inclusive, a primeira menção colegiada, de 2016, externa a repercussão da alteração legislativa quanto à cadeia de custódia.

No AgRg no REsp n. 1.484.986/RS, apesar do argumento defensivo expresso quanto à divergência do código '*hash*' em espelhamento

---

67 ROSA, Gerson Faustino; DUARTE, Myllena Gonçalves. "Crimes de Colarinho Branco: uma análise crítica da seletividade do sistema penal e a incapacidade de enfrentamento das organizações criminosas" in *Revista Eletrônica da Faculdade de Direito de Franca,* v.17, n. 2, 2023.

68 REsp n. 2.150.278/PR, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 24/9/2024, DJe de 27/9/2024 e REsp n. 1.656.348/SP, relator Ministro Paulo de Tarso Sanseverino, Terceira Turma, julgado em 1/12/2020, DJe de 18/12/2020.

69 Nas lições de Ada Pellegrini Grinover, "são de três ordens as mediadas de que dispõe o Estado para impor a observância dos princípios jurídicos em geral", dentre elas as "sanções de caráter repressivo", com o "sistema de nulidades" do processo penal (GRINOVER, Ada Pellegrini. *Liberdades Públicas e Processo Penal* – As Interceptações Telefônicas. São Paulo: Saraiva, 1976, p. 190).

de um HD (*'hard-drive'*), a tese foi rechaçada sob o fundamento do ausente "apontamento da regra legal contrariada na produção probatória". Na oportunidade, a 5ª Turma afirmou que inexistia qualquer "regulamento que discipline de modo expresso o espelhamento de dispositivos" [70].

Mais que a inclusão dos artigos 158-A e seguintes no Código de Processo, os influxos acadêmicos e forenses sobre tema alteraram substancialmente o panorama naquele Tribunal. De 2023, o AgRg no RHC n. 143.169/RJ tem sido repetidamente citado como paradigma do que se espera na cadeia de custódia de evidências digitais.

No caso, a Turma elenca expressamente o algoritmo *'hash'* como ferramenta de comparação à demonstração da integridade e fiabilidade da prova – reconhecendo quebra da cadeia de custódia[71]. Em divergência aberta pelo Min. Ribeiro Dantas, reconheceu-se a "inobservância dos procedimentos técnicos necessários" na arrecadação e armazenamento de arquivos de um computador – mesmo que os fatos (e a colheita da prova) fossem anteriores a 2019.

A partir da doutrina de Geraldo Prado, textualmente referenciado como "um dos impetrantes" do *habeas corpus*, o relator para o acórdão cita a necessária preservação da "mesmidade" com mecanismos objetivos para "aferir a integridade as fontes de prova". E, para afastar a "volatilidade" dos dados, ressaltou que deveria existir a cópia integral "(bit a bit)" com a aplicação da técnica de "algoritmo *'hash'*" com "assinatura única para cada arquivo", "uma espécie de impressão digital ou DNA".

No entanto, ao invés consagrar uma técnica informática ou delimitar a mácula e inadmissibilidade da prova digital a partir de vício no *'hash'*, o que se vê da decisão é a censura processual à falha na "mais básica" providência – ante a documentação inexistente. No caso, a extração foi feita por instituição financeira (vítima) sem mínima documentação da cadeia – cita-se trecho do voto vencedor:

---

[70] STJ, AgRg no REsp n. 1.484.986/RS, relator Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 22/11/2016, DJe de 5/12/2016.

[71] STJ, AgRg no RHC n. 143.169/RJ, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, julgado em 7/2/2023, DJe de 2/3/2023.

> Não existe nenhum tipo de registro documental sobre o modo de coleta e preservação dos equipamentos, quem teve contato com eles, quando tais contatos aconteceram e qual o trajeto administrativo interno percorrido pelos aparelhos uma vez apreendidos pela polícia. Nem se precisa questionar se a polícia espelhou o conteúdo dos computadores e calculou a *hash* da imagem resultante, porque até mesmo providências muito mais básicas do que essa - como documentar o que foi feito - foram ignoradas pela autoridade policial. Chama atenção o fato de que, antes mesmo de ser periciado pela polícia, algo que só aconteceria em novembro de 2017, o conteúdo extraído dos equipamentos foi analisado pela própria instituição financeira vítima, em outubro daquele ano (e-STJ, fls. 468-485).

Assim, em caso posterior de 2024, a própria 5ª Turma rechaçou dissídio jurisprudencial sob alegada contraposição ao decidido no RHC n. 143.169/RJ, assentando a validade de extração com relatório manual, isto é, imagens dos aparelhos celulares apreendidos.

No AgRg no HC n. 829.138/RN, a defesa questionou que, após autorização judicial, os agentes policiais procederam a "análise manual" dos celulares apreendidos – fotografando as telas dos aparelhos e transcrevendo os respectivos diálogos. A Turma, no entanto, rechaçou a tese da identidade com o decidido no RHC n. 143.169/RJ.

"Na hipótese vertente, contudo, o que ocorreu foi a extração de fotografias de tela com dados telemáticos de *Whatsapp* do celular - e não um simples espelhamento ou acesso a conversas do *Whatsapp Web*". Ressaltou que a possibilidade da "perícia técnica com a finalidade de se verificar toda e qualquer alteração da prova", sem a necessidade da extração do *código 'hash'*[72].

A situação fática chancelada não discrepa do argumento trazido no AgRg no HC n. 828.054/RN, com sorte diametralmente distinta. Também após autorização judicial, o delegado acostou relatório dos vestígios encontrados em aparelho celular apreendido com o investigado – ressaltando "a análise foi performada após consulta direta ao aparelho, sem necessidade

[72] STJ, AgRg no HC n. 829.138/RN, relator Ministro Messod Azulay Neto, Quinta Turma, julgado em 6/2/2024, DJe de 14/2/2024.

de uso de máquinas extratoras (ex. *Cellebrite*)". Consequentemente, destacou as capturas de telas e diálogos de interesse da investigação[73].

Desta vez, com voto do Ministro Joel Ilan Paciornik a solução foi pela inadmissibilidade da prova. A decisão introduz o artigo 422, §1º, do Código de Processo Civil, com "diálogo de fontes" [74], afirmando a presunção e validade das imagens digitais – no que se incluem os *'prints'*. Assenta, no entanto, que, uma vez questionado, legitimamente impugnado o conteúdo das supostas conversas do *WhatsApp*, a fiabilidade depende das diretrizes de coleta e armazenamento – com alusão expressa à NBR ISO/IEC 27037/2013.

Em contraposição à decisão antecedente, decidiram que o "acesso direto ao celular apreendido, sem a utilização de ferramenta forense que garantisse a exatidão das evidências" é inadmissível. Citou que, "além da técnica do algoritmo '*hash*', também deve ser utilizado um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos dados do arquivo digital" – referindo, como exemplo, o *software Cellebrite*[75].

As duas decisões referem o RHC n. 143.169/RJ, a doutrina da prova digital de Geraldo Prado, mas, da lavra do mesmo colegiado em meses subsequentes, divergem na conclusão sobre o manuseio do vestígio digital.

Os precedentes do STJ exteriorizam alguma inconsistência e a inobservância de padrões sobre a temática – em especial quando de extrações sem cópia com a autenticação por função *'hash'*.

Exemplificando, a Ministra Daniela Teixeira, em julho de 2024, assentou a violação da cadeia de custódia e a inadmissibilidade pelo manuseio de aparelho celular em "análise preliminar" realizada antes da extração. No RHC n. 188.154/RJ, a Ministra reconhece que, apesar da autorização judicial e "extração completa dos dados" do celular, antes da

---

[73] Relatório de Análise de Aparelho Celular – Extração de Dados - Inquérito Policial n.º 083/2021 no AgRg no HC n. 829.138/RN.

[74] Art. 422 (...) § 1º As fotografias digitais e as extraídas da rede mundial de computadores fazem prova das imagens que reproduzem, devendo, se impugnadas, ser apresentada a respectiva autenticação eletrônica ou, não sendo possível, realizada perícia.

[75] STJ, AgRg no HC n. 828.054/RN, relator Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 23/4/2024, DJe de 29/4/2024.

remessa à inteligência da Polícia para o tratamento técnico, ouve acesso pelos delegados e inspetores, com "fotos da tela do aparelho"[76].

Em decisão mais recente, a Ministra, desta vez no colegiado da 5ª Turma no EDcl no HC n. 945.157/SC, repeliu a tese da quebra da cadeia de custódia e admitidos *'prints'* de mensagens de *WhatsApp* sem autorização judicial, produzidos por "familiar da vítima", porque inexistente "qualquer manipulação indevida". Sem maior fundamentação, a ementa resume a íntegra do fundamento para a admissão da prova, desprovida de qualquer rigor técnico[77].

Realçando a divergência, em processo de organização criminosa, com celulares apreendidos, manuseados por servidores públicos em relatório documentado e posterior perícia, com extração integral da imagem e cálculo da *função 'hash'*, a Ministra reconheceu a quebra da cadeia de custódia, com a mais gravosa sanção processual (desentranhamento da prova). Ante o argumento da possível manipulação pelo delegado e inspetores, mesmo com laudo posterior sobre inexistente indicativo de adulteração, sem "elementos concretos" do que a defesa entendia "terem sido adulterados", apontou a "desconfiança" na prova produzida.

Em contraposição, *'prints'*, sem isolamento, preservação ou documentação, produzidos por "familiar" a partir da captura de tela de conversas entre a vítima e o réu, questionados pelo acusado, foram chancelados, mantida a condenação pelos crimes de estupro de vulnerável e posse de material pornográfico infantil. Neste, foi apontado que as imagens foram extraídas "utilizando ferramentas do próprio aplicativo, sem qualquer manipulação indevida".

Seguindo a temática, o Ministro Reynaldo Soares da Fonseca[78] afastou ilicitude da prova consistente em vídeos extraídos sem ficha do

---

[76] STJ, RHC n. 188.154/RJ, Ministra Daniela Teixeira, julgado em 24/07/2024.

[77] "(...) 4. As provas obtidas mediante prints de WhatsApp não configuram violação à cadeia de custódia, tendo em vista que foram realizadas por familiar da vítima, utilizando ferramentas do próprio aplicativo, sem qualquer manipulação indevida. Além disso, tanto a vítima quanto o réu confirmaram a troca de mensagens" (EDcl no HC n. 945.157/SC, relatora Ministra Daniela Teixeira, Quinta Turma, julgado em 4/11/2024, DJe de 6/11/2024).

[78] STJ, HC n. 901.602/PB, Ministro Reynaldo Soares da Fonseca, julgado em 08/11/2024.

vestígio e '*hash*' na extração da origem. Na decisão, realçou a distinção aos precedentes citados em que se sancionou as hipóteses "sem qualquer observância à cadeia de custódia" (AREsp n. 2.342.908/MG) ou, como no 143.169/RJ, cm que remetidos os vestígios para a instituição vítima.

Na decisão, ainda, o Ministro trouxe destaque à doutrina de Clarissa Diniz Guedes da admissibilidade das provas em vídeo – que traz algumas luzes que podem se estender em relação a outras provas e vestígios digitais:

> *(...) nas palavras de Clarissa Diniz Guedes, "Idealmente, para fins criminais, a obtenção da prova em vídeo deveria partir do vídeo original ou uma cópia perfeita (p. ex. com código* hash*), no mesmo formato do vídeo original. Todavia, não se pode descartar a possibilidade de que o vídeo seja apresentado em outro formato, ainda que com algum grau de compactação, mas que, ainda assim permita a análise da integridade das imagens". Ainda segundo a autora: "Neste* último *caso, todavia, haverá a necessidade de esclarecimentos técnicos sobre eventuais limitações da aferição da integridade, tanto para o fim de se confirmar que a integridade possa ser atentada com um grau de fiabilidade mínimo, como para esclarecer sobre as limitações dessa aferição, que eventualmente impactarão no exame da eficácia probante do vídeo, levando em conta o contexto probatório" (Guedes, Clarissa Diniz. Prova em vídeo no processo penal: aportes epistemológicos. Rio de Janeiro: Marcial Pons, 2023, p. 47).*

Com efeito, reconhecida que a posterior submissão à perícia, com o cálculo '*hash*' e a disponibilidade da íntegra dos arquivos (inclusive da respectiva documentação da custódia) suprem a exigência do Código de Processo Penal, invocando jurisprudência longeva de que "não se pode presumir eventual má-fé dos agentes públicos no manuseio das provas"[79]. E conclui que "não haveria se falar em nulidade, mas apenas em menor ou maior confiabilidade da prova, porquanto não indicada a prática de qualquer conduta que pudesse revelar a manipulação das imagens, a ponto de torná-las provas ilícitas".

[79] STJ, AgRg no AREsp n. 2.511.249/MG, relator Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 15/10/2024, DJe de 17/10/2024.

No RHC n. 203.749, monocraticamente, o Ministro Ribeiro Dantas manteve decisão do Tribunal de Justiça do Estado de São Paulo que declarou "desnecessária" a função '*hash*' em arquivos extraídos do 'Sistema Guardião' que armazena as interceptações telefônicas redistribuídas pelas operadoras de telefonia. O acórdão da origem transcrito decidiu que os dados do sistema já são "protegidos por criptografia e/ou senha", dificultando a alteração; o que foi reputado como "explicação" satisfatória para refutar o revolvimento da prova no STJ[80]. Igualmente do Ministro Ribeiro Dantas, a advertência de que a "simples existência da '*hash*' não permite concluir que o arquivo apresentado é autêntico e íntegro"[81].

Neste sentido, a Ação Penal n. 623, talvez represente o mais consolidado entendimento sobre o tema por colegiado do STJ. Na oportunidade, a Corte Especial enfrentou o tema do '*hash*', definindo-o e reconhecendo sua relevância, mas a dispensa para a auditabilidade de interceptações telefônicas já sob *software* próprio com propósito semelhante (Guardião). Ressalta que "a ausência de geração de código '*hash*', por si só, não é apta a invalidar as provas colhidas"[82].

3.2 Parâmetros Técnicos e Jurídicos da Integridade da Prova Digital

Sob tais premissas técnicas, com as preocupações sobre o recorte de processos e a divergência evidente sobre o tema, possível extrair diretrizes e parâmetros para a garantia da integridade dos vestígios e provas digitais com (ou sem) o emprego da função '*hash*'.

De plano, cognoscível conteúdo comum e subjacente às decisões sobre a temática: a imperativa documentação da cadeia de custódia.

Além da previsão dos artigos 158-A e seguintes do Código de Processo Penal, o registro detalhado da cadeia de custódia é um dever para o "controle epistêmico"[83] da prova. "Exige o estabelecimento de um

---

[80] STJ, RHC n. 203.749, Ministro Ribeiro Dantas, DJe de 17/12/2024.

[81] STJ, RHC n. 205.088, Ministro Ribeiro Dantas, DJe de 20/12/2024.

[82] STJ, APn n. 623/DF, relator Ministro Francisco Falcão, Corte Especial, julgado em 4/6/2025, DJe de 16/6/2025.

[83] PRADO, Geraldo. *Prova Penal e Sistema de Controles Epistêmicos* – a quebra da cadeia de custódia das provas obtidas por métodos ocultos, 1ª ed. São Paulo:

procedimento regrado e formalizado, documentando toda a cronologia existencial daquela prova, para permitir posterior validação em juízo e exercício do controle epistêmico"[84].

Seja qual for o método, a tecnologia empregada ou a natureza da prova, é necessária mínima documentação. Sendo a prova digital "imaterial", "dispersa" e "instável", "o investigador deverá munir-se de todas as técnicas e conhecimentos científicos", o que exige a "cumulação dos princípios probatórios do processo penal e da investigação forense"[85].

Tais características impõem maior rigor na documentação, que deve ser "detalhada" – cogitável até o registro em vídeo de toda a operação e os passos da continuidade e definição da cadeia de custódia[86]. É a "história cronológica escrita, ininterrupta e testemunhada, de quem teve a evidência desde o momento da coleta até que ela seja apresentada"[87].

Por outro lado, a "mera possibilidade" da modificação ou alteração da prova digital não é suficiente para a "excluir" do âmbito penal, com necessária análise tópica da confiabilidade e do valor demonstrativo da prova[88].

Marcial Pons, 2014.

84 JUNIOR, Aury Lopes. *Direito Processual Penal* - 21ª Edição. Rio de Janeiro: Saraiva, 2024. E-book. p.479

85 CANCELA, Alberto Gil. *A Prova Digital*: os meios de obtenção de prova na lei do cibercrime (Dissertação de Mestrado). Faculdade de Direito, Universidade de Coimbra, orient. Sonia Mariza Florêncio Fidalgo, 78p, Coimbra, 2016, pp. 22-23.

86 Idem, p. 954.

87 BADARÓ, Gustavo. A cadeia de custódia e sua relevância para a prova penal. In: SIDI, Ricardo; LOPES, Anderson Bezerra (orgs.). *Temas Atuais da investigação preliminar no processo penal*. Belo Horizonte, D'Plácido, 2018, p. 522.

88 Tradução livre de "La mera possibilità che sia stata modificata o alterata non è un motivo suffi- ciente per escluderla, fermo restando il giudizio caso per caso sull'attendibilità e sul valore dimostrativo della prova. In ogni caso la prova digitale apre scenari inediti, sia per le caratteristi- che strutturali, sia per le enormi potenzialità che offre alle indagini. Ormai la maggior parte degli atti di indagine presenta una componente digitale" (ILLUMINATI, Giulio. "Prova Digitale e Ammissibilità" in VALENTE, Manuel Monteiro Guedes; WUNDERLICH, Alexandre (orgs.). *Direito e Liberdade* – Estudos em homenagem ao Professor Doutor Nereu José Giacomolli. São Paulo: Almedina, 2022, p. 948).

Exatamente da conjugação dos princípios forenses e jurídicos, a função '*hash*' surge como relevante ferramenta da "prova da prova", apta a gerar presunção (relativa) da satisfação do ônus do Estado na documentação da cadeia de custódia – mas, não mais que isso. O '*hash*' não serve a todo e qualquer dado, tampouco se mostra útil a gênero indistinto de evidências digitais.

Ao contrário de reputá-lo dispensável, irrelevante ou inseguro, o código '*hash*' tem específica utilidade na fiabilidade e integridade da prova digital. Contudo, consagrá-lo sem o rigor científico forense pode chancelar mero engodo de tecnicismo sobre a prova digital – fomentando críticas já recorrentes de insegurança jurídica, seletividade e discricionariedade.

"Imprescindível que o método empregado garanta a integridade do dado digital"[89]. A confiabilidade da informação "depende de mecanismos técnicos que garantem a integridade, a inalterabilidade, a rastreabilidade, a recuperabilidade e a conservação"[90]. Normativas de padronização e regulamentação de protocolos sugerem alguns mecanismos, que, entretanto, devem ser avaliados segundo os limites ínsitos à tecnologia e ao avanço digital. Reitera-se a preocupação:

> *(...) as peculiaridades da prova científica podem colocar em crise a relação tradicional entre prova e julgamento, ao implicar um raciocínio probatório que necessariamente deve se apoiar em regras científicas desconhecidas para os juízes, como ferramenta para acessar um fato desconhecido a partir de um fato conhecido. Pois bem, na 'novel science', o método científico utilizado pode ainda não ter sido submetido à crítica de toda a comunidade científica ou, então, pode ainda não ter tido aplicação jurisprudencial: daí o risco de ingresso indiscriminado no processo penal de formas questionáveis de 'junk science'*[91].

---

[89] BADARÓ, Gustavo. "Os standards metodológicos de produção da prova na prova digital e a importância da cadeia de custódia" in *Revista IBCCRIM*, São Paulo, v. 343, ano 29, p. 7-9, jun./2021, p. 8.

[90] BUJOSA VADELL, Lorenzo M.; BUSTAMANTE RÚA, Mónica M.; TORO GARZÓN, Luis O. La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, vol. 7, n. 2, p. 1347-1384, mai./ago. 2021, p. 1367.

[91] "En efecto, las peculiaridades de la scientific evidence pueden poner en crisis la relación tradicional entre prueba y juicio, al implicar un razonamiento

Consenso que a extração *'bit a bit'*, "autenticada pelo código *'hash'*" integra as "melhores práticas"[92], o que não exclui outras alternativas, nem afasta o necessário zelo da técnica empregada. A extração de imagem não é uma realidade possível ou viável em todo de repositório digital ou aparelho eletrônico. Nem mesmo os mais avançados e consagrados *hardwares* e *softwares* para a extração de mídias digitais podem assegurar êxito; há resultados distintos em determinados sistemas operacionais ou métodos de encriptação da origem dos dados[93].

A cópia forense recomenda técnica com os "mais altos padrões possíveis", o que não exclui situações peculiares. As diretrizes não abrangem todo gênero de eventualidades; o banco de dados de uma instituição financeira em alteração constante e volume armazenado em uma "sala do tamanho de um campo de futebol" não está contemplado[94], o que não impede tal prova. Assim como *'print'* de uma conversa produzida informalmente por familiar da vítima em hipótese recém-chancelada pelo STJ, a integridade perpassa mais que o cálculo *'hash'*.

Ao contrário de um pretenso "efeito dissuasório" com a imposição de um "padrão de legalidade"[95], ainda que necessário "estigmatizar

---

probatorio que necesariamente debe apoyarse en leyes científicas desconocidas para los jueces, como herramienta para acceder a un hecho desconocido a partir de un hecho conocido. Ahora bien, en la novel science, el método científico utilizado podría no haber sido sometido aún a la crítica de toda la comunidad científica, o bien podría no haber tenido aún aplicación jurisprudencial: de ahí el riesgo de ingreso indiscriminado en el proceso penal de formas discutibles de junk science" (MARAFIOTI, Luca. "Prueba Digital y Proceso Penal" in *Revista de Derecho Penal y Proceso Penal*, n. 11, nov./2012, pp. 1904-1912,

92 GUERRA, Maite Neves. *Regime Democrático das Provas Digitais no Processo Penal: aquisição e qualificação* (Dissertação de Mestrado), Universidade do Vale do Itajaí, 169p., Itajaí, 2024, p. 124.

93 AFONIN, Oleg; KATALOF, Vladimir. *Mobile Forensics* – Advanced Investigative Strategies. Birmingham: Packt, 2016, p. 125 e ss; REIBER, Lee. *Mobile Forensic Investigations*: A Guide to Evidence Collection, Analysis and Presentation, 1a ed. McGraw Hill, 2015

94 MASON, Stephen; SHELDON, Andrew; DRIES, Hein. "Proof: The Technical collection and examination of electronic evidence" in MASON, Stephen; SENG, Daniel. *Electronic Evidence and Electronic Signatures,* v. 5. Londres: University of London Press, 2021, p. 295.

95 JUNIOR, Aury Lopes. *Direito Processual Penal,* 21ª ed. Rio de Janeiro: Saraiva Jur, 2024. *E-book*. p.482.

a negligência"[96] da cadeia de custódia, estabelecer fórmulas simplistas arrisca o estabelecimento de um *'standard'* pouco crível, utópico, e fomenta (mais) a seletividade criminal.

Ainda que as provas digitais exijam a observância das "*best practices* nacionais e internacionais" para o "potencial epistêmico adequado"[97], não se pode conceber a interpretação da reconstituição da cadeia de custódia exclusivamente por prova pericial "esse meio não é o único adequado ou obrigatório para todos os casos"[98]. O "problema das provas ilícitas" não se confunde com o "conteúdo e a veracidade" da prova que se projetam para o plano da valoração[99]; exigindo-se da cadeia de custódia o suficiente para "suplantar dúvidas razoáveis"[100].

Muito antes da discussão prova digital, em proposta de sistematização genérica da liberdade probatória, Eugenio Florian já mencionava "exigências substanciais", dentre as quais a "utilização de dados científicos" quando possível[101]. Em sentido análogo, não é possível supor a imposição indiscriminada da tecnologia sem o rigor técnico próprio da ciência forense, muito menos consagrar o código *'hash'* como ferramenta exclusiva na satisfação da cadeia de custódia.

Mesmo sob o rigor e cuidado da prova digital, "ao menos que a exclusão" seja lastreada em violação de procedimento "expressamente previsto em lei", a "eventual violação das boas práticas incide somente

---

96 BARTOLI, Laura. *La catena di custodia del materiale informatico*: soluzioni a confronto, 2016. Anales de la Facultad de Derecho,33, 2016. Bologna: Facultad de Derecho, diciembre 2016. p. 145-162. p. 162.

97 BADARÓ. Os *standards*... Ob. cit., p. 9.

98 CARDOSO, Oscar Valente. Dados e metadados, provas e metaprovas: as provas sobre as provas digitais. *Revista de Direito e as Novas Tecnologias*. vol. 21. ano 6. São Paulo: Ed. RT, out.-dez. 2023.

99 GRINOVER, Ada Pellegrini; FERNANDES, Antônio Scarance; GOMES FILHO, Antônio Magalhães. *As Nulidades no Processo Penal*, 9ª ed. rev. atualizada e ampliada. São Paulo: Revista dos Tribunais, 2006, p. 151.

100 EDINGER, Carlos. Cadeia de Custódia, Rastreabilidade Probatória. *Revista Brasileira de Ciências Criminais*, vol. 120, p. 237-257, maio – junho 2016.

101 FLORIÁN, Eugenio. *De Las Pruebas Penales*, Tomo I, De La Prueba en General, 2ª reimpressão, 3ª ed. Santa Fé de Bogotá: Temis, 1995, p. 316-321; DEZEM, Guilherme Madeira. *Curso de Processo Penal*, 1ª ed. São Paulo: Revista dos Tribunais, 2015, p. 545.

na valoração da prova"[102]. Não obstante o especial zelo que as evidências digitais devem inspirar, ilidível que o "direito processual clássico fornece ferramentas de investigação que se revelam muito úteis à obtenção de prova no ambiente digital"[103].

Nem sempre é necessária a extração da imagem *'bit a bit'*; às vezes, nem será possível; de igual modo, a função *'hash'* talvez não seja o melhor protocolo para determinados arquivos (ex. páginas URL). Assim, excetuadas as hipóteses acertadamente sancionadas com a ilicitude e inadmissibilidade, em razão da falta de mínima documentação da cadeia de custódia, ordinariamente, a prova digital está sujeita às normas 'clássicas' de admissibilidade.

Destacando que os "meios ordinários usados para verificar a autenticidade dos documentos não se aplicam às provas informáticas", Michele Taruffo registra que deixar à "valoração discricionária do julgador pode parecer uma forma de evadir-se do problema"[104]. O que revelam os precedentes destacados do Superior Tribunal de Justiça, no entanto, é que, sob as premissas do que se considera a "melhor prática" ou sob mais rigorosos protocolos da fiabilidade tecnológica vigentes, é panorama de igual discricionariedade e insegurança jurídica.

Igualmente, se a "mera" existência do *'hash'* não basta à integridade da prova digital, com já afirmado pelo STJ, a comparação e divergência tampouco pode ser interpretada de forma inequívoca para a inadmissibilidade do arquivo.

Invocar a técnica demanda sensibilização coletiva e "alfabetização" das partes do processo[105]. A existência de *'hash'* não significa mais que a

---

[102] ILLUMINATI, Giulio. "Prova Digitale e Ammissibilità" in VALENTE, Manuel Monteiro Guedes; WUNDERLICH, Alexandre (orgs.). *Direito e Liberdade* – Estudos em homenagem ao Professor Doutor Nereu José Giacomolli. São Paulo: Almedina, 2022, p. 956.

[103] VERDELHO, Pedro. "A obtenção de prova no ambiente digital" in Revista do Ministério Público de Lisboa, Lisboa, v. 25, n. 99, p. 117-136, jul./set. 2004. Disponível em: <http://201.23.85.222/biblioteca/index.asp?codigo_sophia=49232>. Acesso em 21/10/2024.

[104] TARUFFO, Michele. *A Prova*, trad. João Gabriel Couto, Filosofia e Direito. São Paulo: Marcial Pons, 2014, p. 85/87.

[105] BARTOLI, Laura. *La catena di custodia del materiale informatico*: soluzioni a confronto, 2016. Anales de la Facultad de Derecho,33, 2016. Bologna:

submissão de um arquivo ou pacote de dados a um cálculo matemático. Só que, mais que compará-lo ou confrontá-lo, é preciso compreender as suas características para avaliar o melhor protocolo/função, a coincidência frente aos riscos de colisão ou eventual divergência.

Ilustrando, há muito, especialistas em criptografia consideram a função '*hash*' MD5 um protocolo obsoleto, inseguro, o que pode ser considerado "prejudicial" ou "problemático" na pretensa definição da fiabilidade[106]. Não por acaso, a melhor técnica consiste na solução de combiná-lo com outros protocolos (ex. SHA), afastando o risco de colisão proposital em razão da redundância que tornaria bastante complexa a colisão dupla[107].

De outro modo, por sua natureza e complexidade, a submissão de pacotes a mais de um protocolo significa maior tempo e demanda tecnológica de processamento computacional. E, por óbvio, incrementa riscos de erros, o que é próprio de qualquer procedimento técnico-científico[108].

Facultad de Derecho, diciembre 2016. p. 162.

[106] KAMINSKY, Dan. MD5 to be considered harmful someday. *IACR Cryptology ePrint Archive*, 2004. Disponível em: <https://eprint.iacr.org/2004/357.pdf>. Acesso em 24 dez. 2024.

[107] "Utilizzare più funzioni è uno stratagemma per aumentare la sicurezza dell'identificazione: come dicevamo, è improbabile —sebbene possibile— che due input diversi diano luogo alla stessa traccia *hash*. Il rischio che la difformità tra originale e copia passi inosservata utilizzando due diversi algoritmi è addirittura inverosimile: anche se si verificasse una collisione rispetto a uno dei due risultati, l'altro supplirebbe" (BARTOLI, Laura. *La catena di custodia del materiale informatico*: soluzioni a confronto, 2016. Anales de la Facultad de Derecho,33, 2016. Bologna: Facultad de Derecho, diciembre 2016. p. 156). Em sentido contrário, apontando a "insuficiência" da combinação dos protocolos MD5 e SHA1 ("MD5 and SHA1 *hashes* are insufficient to ensure the integrity of the evidence" – ELGOHARY, Hany M; DARWISH, Saad M.; ELKAFFAS, Saleh Mesbah. "Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications" in *IEEE Access*, v. 10, fevereiro/2022, p. 14669-14678. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9698053>. Acesso em 04/01/2025).

[108] AMARAL, Maria Eduarda Azambuja; BRUNI, Aline Thais. Prova Pericial no Processo Penal: a compreensão e a mitigação dos erros forenses como mecanismo de respeito ao contraditório, à ampla defesa e ao direito à prova lícita. *Revista Brasileira de Direito Processual Penal*, v. 9, n. 2, pp. 877-912, Porto Alegre, maio-ago./2023, p. 889. Disponível em: <https://doi.org/10.22197/rbdpp.v9i2.819>. Acesso em 04/01/2025.

Não à toa, a técnica forense mais atual recomenda a conjugação de protocolos e o particionamento dos vestígios – com a produção de *'hashes' difusos* (*'fuzzy hashes'*), como "nova técnica" para determinar a "similaridade" de arquivos, como nos dados com algumas estruturas especialmente voláteis e não controláveis[109].

Os métodos de criptografia e a evolução do processamento computacional, por sua natureza, recomendam que se deve "sempre migrar para um novo algoritmo" mais atual e seguro[110]. A possibilidade de colisões com menor esforço a cada dia[111], denota a presunção relativa da integridade a partir da juntada do código *'hash*' e sugere a necessidade de evolução constante, análise tópica da integridade e fiabilidade, sem soluções automáticas ou regras desarrazoadas.

4. CONCLUSÃO

Como ressalta Paulo Victor Alfeo Reis, "o sistema normativo não está apto a acompanhar a velocidade de mudanças de hábito de um mundo tão disruptivo" como o das relações algorítmicas e nunca "o Judiciário foi tão relevante para dar segurança jurídica em uma realidade cada vez mais rápida"[112]. Ao mesmo tempo, com frequência cada vez mais acentuada, submete-se à jurisdição demandas de maior complexidade "científica

---

[109] ELGOHARY, Hany M; DARWISH, Saad M.; ELKAFFAS, Saleh Mesbah. "Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications" in *IEEE Access*, v. 10, fevereiro/2022, p. 14670.

[110] PRADEEP, K. C.; SOMAN, Rajashree; HONNAVALLI, Prasad. "Validity of Forensic Evidence Using *Hash* Function" in *Proceedings of the Fifth International Conference on Communication and Electronics Systems* (ICCES 2020), IEEE Conference Record # 48766, 2020, p. 826. Disponível em: <https://ieeexplore.ieee.org/document/9138061/>. Acesso em 03/01/2024).

[111] RASJID, Zulfany Erlisa; SOEWITO, Benfano; WITJAKSONO, Gunawan; ABDURACHMAN, Edi. A review of collisions in cryptographic *hash* function used in digital forensic tools. *Procedia Computer Science*, v. 116, p. 381-392, 2017. Disponível em: <https://doi.org/10.1016/j.procs.2017.10.072>. Acesso em 24 dez. 2024.

[112] REIS, Paulo Victor Alfeo. *Algoritmos e o Direito*. São Paulo: Almedina, 2020, p. 147.

e técnica" – que exigem "conhecimentos altamente especializados e particulares"[113].

Neste contexto, surge o desafio probatório e a discussão sobre a integridade e fiabilidade das evidências digitais. Embora não contemplado expressamente nas regras da cadeia de custódia elencadas no Código de Processo Penal, expresso em manuais, guias e diretrizes de boas práticas forenses, o código *'hash'* tem sido citado como instrumento de garantia da autenticidade e integridade dos vestígios na demonstração da cadeia de custódia.

A adoção irrefletida da tecnologia, sem rigor científico ou conhecimento técnico, tem a mesma relevância para o controle epistêmico da prova penal que o emprego de método nenhum. Buscou-se neste ensaio expor premissas, fundamentos científicos e argumentos jurídicos que permitam refletir diretrizes e parâmetros para a garantia da integridade do vestígio digital. De forma resumida, possível estabelecer alguns tópicos que reúnem tais parâmetros:

a) Documentação rigorosa: atender à exigência do Código de Processo Penal, em prestígio à integridade e racionalidade para a valoração posterior da prova digital, pressupõe a observância de um mínimo rigor na documentação, com o registro detalhado da cadeia de custódia. E a exigência da documentação consiste em filtro (mínimo) para a admissibilidade do vestígio digital como prova.

b) Limites da legislação e normatização: a evolução tecnológica torna inviável a padronização ou pormenorização da prova digital no âmbito legislativo, reconhecendo ao capítulo da cadeia de custódia do Código de Processo Penal a função vetor interpretativo na constante atualização dos métodos e padrões consagrados na ciência forense para o tratamento, preservação e integridade dos vestígios digitais – realçando a importância do emprego de melhores técnicas como aquelas das normas da ABNT ISO/IEC 27037:2013 ou RFC 3227, que não afastam outros métodos e técnicas.

[113] DAMASKA, Mirjan R. *El Derecho Probatorio a la Deriva* – Processo y Derecho, trad. Joan Picó i Junoy. Madrid: Marcial Pons, 2015, p. 147.

c) '*Hash*': a função '*hash*' é um algoritmo matemático calculado em pacote de dados digitais que resume o arquivo em uma saída padrão hexadecimal única, cuja comparação pode confirmar a integridade, em razão de sua natureza determinística. Tecnologia versátil, ostenta diversos protocolos e métodos que podem ser avaliados segundo conveniência de processamento de dados, tempo, segurança e extensão (ex. MD4, MD5, SHA-1, SHA-256, SHA-512 etc.).

d) Limites do '*hash*': exatamente pela natureza determinística que lhe torna relevante à finalidade da cadeia de custódia, nem sempre será útil ou viável o cálculo de um código '*hash*' em determinados arquivos, sem conferência viável ou relevante. Novos métodos que recomendam fracionamento e cálculos múltiplos de parcelas do conteúdo, a demonstrar a similaridade, afastando o risco de erros periciais e vícios da manipulação não intencional ou irrelevante para integridade do vestígio.

e) Avanço tecnológico e '*hash*': baseado na premissa da dificuldade da inversão do cálculo e *colisão*, o algoritmo '*hash*' pode se tornar obsoleto ou inseguro com a evolução do processamento computacional. Determinados modelos já são considerados superados em ferramentas de segurança da informação e criptografia, com recomendável emprego combinado de métodos e protocolos a garantir a fiabilidade do vestígio a partir da redundância.

f) Presunção de integridade: reconhecida dentre as melhores técnicas, a extração *'bit a bit'* de um arquivo com o cálculo conferível e confirmado de coincidência do '*hash*' gera presunção de integridade e fiabilidade do vestígio. A inexistência, "colisão" ou não conferência do código '*hash*', de outro modo, deve ser avaliada de forma tópica no plano da valoração probatória, com a premissa mínima da documentação como filtro de admissibilidade do vestígio.

g) Educação e preocupação com a técnica: seja pelos limites ínsitos da tecnologia, seja pelo risco da sua falibilidade, o tratamento da prova digital e emprego da função '*hash*' pressupõem

educação e sensibilização das partes envolvidas no processo sobre o rigor científico e conhecimento exigido, afastando teses extremas, com *'standards'* utópicos ou a admissão de elementos sem mínima fiabilidade.

Embora "valioso"[114], o código *'hash'* não é infalível e não pode ser aplicado a todos os processos ou espécies de dados. O algoritmo não supre todos os desafios sobre a admissibilidade os vestígios digitais, suas limitações ínsitas pela natureza determinística ou inseguranças pela evolução tecnológica expõem os riscos da consagração de uma ferramenta que deve ser interpretada como tal – mais um instrumento que renova o diálogo próprio do processo penal e a racionalidade na valoração das provas.

REFERÊNCIAS

AFONIN, Oleg; KATALOF, Vladimir. *Mobile Forensics* – Advanced Investigative Strategies. Birmingham: Packt, 2016.

ALCOCEBA GIL, Juan Manuel. Los estándares de cientificidad como criterio de admisibilidad de la prueba científica. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 4, n. 1, p. 215-242, jan./abr. 2018. https://doi.org/10.22197/rbdpp.v4i1.120.

AMARAL, Maria Eduarda Azambuja; BRUNI, Aline Thais. Prova Pericial no Processo Penal: a compreensão e a mitigação dos erros forenses como mecanismo de respeito ao contraditório, à ampla defesa e ao direito à prova lícita. *Revista Brasileira de Direito Processual Penal*, v. 9, n. 2, pp. 877-912, Porto Alegre, maio-ago./2023. <https://doi.org/10.22197/rbdpp.v9i2.819>.

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2024. São Paulo: Fórum Brasileiro de Segurança Pública, ano 18, 2024.

ARSLAN, Engin; ALHUSSEN Ahmed. "Fast integrity verification for high-speed file transfers" in *arXiv preprint arXiv:1811.01161*, 2018. Disponível em: <https://arxiv.org/pdf/1811.01161>.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27037:2013*. Rio de Janeiro: ABNT, 2013.

[114] LORDELO, João Paulo. *Constitucionalismo Digital e Devido Processo Legal*, 2ª ed. Revista e atualizada. São Paulo: JusPodivm, 2024, p. 326.

ATURBAN, Mohamed; NELSON, Michael L.; WEIGLE, Michele C. Difficulties of Timestamping Archived Web Pages. *arXiv preprint arXiv:1712.03140*, 2017. Disponível em: <https://arxiv.org/abs/1712.03140>.

BADARÓ, Gustavo. A cadeia de custódia e sua relevância para a prova penal. In: SIDI, Ricardo; LOPES, Anderson Bezerra (orgs.). *Temas Atuais da investigação preliminar no processo penal*. Belo Horizonte, D'Plácido, 2018.

BADARÓ, Gustavo. Os *standards* metodológicos de produção da prova na prova digital e a importância da cadeia de custódia. *Revista IBCCRIM*, São Paulo, v. 343, ano 29, p. 7-9, jun./2021. Disponível em: <https://www.publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325>.

BARTOLI, Laura. La catena di custodia del materiale informatico: soluzioni a confronto. *Anales de la Facultad de Derecho*, 33, Bologna, 2016..

BENTHAM, Jeremias. *Tratado de las pruebas judiciales* – Tomo I, tradução de Dom José Gomez de Castro. Madrid: Imprenta de D. Tomás Jordan, 1835.

BIHAM, E., CHEN, R., JOUX, A. et. al. Collisions of SHA-0 and Reduced SHA-1. In: CRAMER, R. *Advances in Cryptology* – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Berlin: Springer, 2005, disponível em: <https://doi.org/10.1007/11426639_3>.

BUJOSA VADELL, Lorenzo M.; BUSTAMANTE RÚA, Mónica M.; TORO GARZÓN, Luis O. La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, vol. 7, n. 2, p. 1347-1384, mai./ago. 2021. https://doi.org/10.22197/rbdpp.v7i2.482.

CANCELA, Alberto Gil. *A Prova Digital*: os meios de obtenção de prova na lei do cibercrime. Dissertação – Faculdade de Direito, Universidade de Coimbra, Coimbra, 2016. Disponível em: <https://hdl.handle.net/10316/31398>.

CANTALI, Fernanda Borghetti. *A Tokenização da Arte Visual e o Direito Autoral*: o Copyright by Design e a definição das premissas mínimas de governança para viabilizar o NFT – Non Fungible Token como instrumento de negociação de obras de arte. Brasil: Editora Dialética, 2024.

CASEY, Eoghan. *Digital Evidence and Computer Crime*: Forensic Science, Computers and the Internet. 3a ed. Burlington: Elsevier, 2011.

CASTELLS, Manuel. *Fim de Milênio* – A Era da Informação – Economia, Sociedade e Cultura, v. 3. Trad. Klauss Brandini Gerhardt e Roneide Venancio Majer, 7ª ed. Rio de Janeiro: Paz e Terra, 2020.

CARDOSO, Oscar Valente. Dados e metadados, provas e metaprovas: as provas sobre as provas digitais. *Revista de Direito e as Novas Tecnologias*. vol. 21. ano 6. São Paulo, out.-dez. 2023.

COSTA, Arthur Trindade Maranhão; DE OLIVEIRA JUNIOR, Almir. Novos padrões de investigação policial no Brasil. In: *Sociedade e Estado*, v. 31, n. 1, p. 147–164, 2016. Disponível em: <https://periodicos.unb.br/index.php/sociedade/article/view/6083>..

COUTINHO, Severino. *Criptografia*. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada, 2016.

DAMASKA, Mirjan R. *El Derecho Probatorio a la Deriva* – Processo y Derecho, trad. Joan Picó i Junoy. Madrid: Marcial Pons, 2015.

DANIELE, Marcello. La Prova Digitale nel Processo Penale. *Rivista di Diritto Processuale*, n. 2, mar.-abr.-2011.

DEZEM, Guilherme Madeira. *Curso de Processo Penal*, 1ª ed. São Paulo: Revista dos Tribunais, 2015.

DIFFIE, Whitfideld; HELLMAN, Martin E. New Directions in Cryptography. *IEEE Transactions on Information Theory*, Vol. IT22, n° 6, pp. 644-654, novembro de 1976.

DURANTI, Luciana; STANFIELD, Allison. Authenticating electronic evidence. In: MASON, Stephen; SENG, Daniel (Ed.). *Electronic evidence and electronic signatures*. CMB-Combined volume, v. 5. London: University of London Press, 2021. Disponível em: <http://www.jstor.org/stable/j.ctv1vbd28p.13>.

EDINGER, Carlos. Cadeia de Custódia, Rastreabilidade Probatória. *Revista Brasileira de Ciências Criminais*, vol. 120, p. 237-257, maio – junho 2016.

ELGOHARY, Hany M; DARWISH, Saad M.; ELKAFFAS, Saleh Mesbah. Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications. *IEEE Access*, v. 10, fevereiro/2022, p. 14669-14678. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9698053>.

ESPIÑEIRA, Bruno; et al. *A prova e o processo penal constitucionalizado:* estudos em homenagem ao ministro Sebastião Reis. Belo Horizonte: Editora D´Placido, 2021.

FISBERG, Yuri. Dataset de "Função '*hash*' e a integridade da prova digital". *SciELO Data*, V1, 2025. https://doi.org/10.48331/scielodata.T2RHA3

FLORIÁN, Eugenio. *De Las Pruebas Penales*, Tomo I, De La Prueba en General, 2ª reimpressão, 3ª ed. Santa Fé de Bogotá: Temis, 1995.

GOMES, Liliane Estela. *Afastamento da Súmula 7/STJ em recursos envolvendo discussão sobre a prova pericial em ações de reparação de danos:* análise de casos concretos. Dissertação – Fundação Getúlio Vargas, São Paulo, 2020.

GOMES, Luiz Flávio Gomes. A impunidade da macrodelinquência econômica desde a perspectiva criminológica da teoria da aprendizagem. *Letras Jurídicas Revista Eletrónica de Derecho del Centro Universitario de la Ciénega*, n. 12, 2011, p. 07. Disponível em: <http://letrasjuridicas.cuci.udg.mx/index.php/letrasjuridicas/article/view/128/126>.

GRINOVER, Ada Pellegrini; FERNANDES, Antônio Scarance; GOMES FILHO, Antônio Magalhães. *As Nulidades no Processo Penal*, 9ª ed. rev. atualizada e ampliada. São Paulo: Revista dos Tribunais, 2006.

GRINOVER, Ada Pellegrini. *Liberdades Públicas e Processo Penal* – As Interceptações Telefônicas. São Paulo: Saraiva, 1976.

GUERRA, Maite Neves. *Regime Democrático das Provas Digitais no Processo Penal:* aquisição e qualificação. Dissertação – Universidade do Vale do Itajaí, Itajaí, 2024.

HASHIM, Hasan; ALZIGHAIBI, Ahmad Reda; ELESSAWY, Amaal Farag [et. al.]. Securing Financial Transactions with a Robust Algorithm: Preventing Double-Spending Attacks. *Computers* 12, n. 9: 171, 2023. Disponível em: <https://doi.org/10.3390/computers12090171>.

ILLUMINATI, Giulio. Prova Digitale e Ammissibilità. In: VALENTE, Manuel Monteiro Guedes; WUNDERLICH, Alexandre (orgs.). *Direito e Liberdade* – Estudos em homenagem ao Professor Doutor Nereu José Giacomolli. São Paulo: Almedina, 2022.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). *Censo 2022*, Panorama Brasil. Brasília: IBGE, 2022. Disponível em: <https://censo2022.ibge.gov.br/panorama/>.

INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL. *Manual do Usuário para registro eletrônico de Programas de Computador*. Diretoria de Patentes, Programas de Computador e Topografias de Circuitos Integrados. Helmar Alvares, Antônio Carlos Coelho e Matheus Souza Pinto Engel. Rio de Janeiro: INPI, 2022.

INTERNET ENGINEERING TASK FORCE (IETF). *Guidelines for Evidence Collection And Archiving,* Network Working Group, D. Brezinski, Best Current Practice, fev. 2002. Disponível em: <https://www.rfc-editor.org/rfc/pdfrfc/rfc3227.txt.pdf>.

KAMINSKY, Dan. MD5 to be considered harmful someday. *IACR Cryptology ePrint Archive*, 2004. Disponível em: <https://eprint.iacr.org/2004/357.pdf>.

KAUFMANN, Alex; GARTMON, Emelie. *Comparative Analysis of Different Cryptographic* Hash *Functions,* Degree Project in Technology, KTH Royal Institute of Technology, Stockholm, 2024. Disponível em: <https://kth.diva-portal.org/smash/get/diva2:1885074/FULLTEXT01.pdf>.

KERR, Orin S. Digital Evidence and the New Criminal Procedure. *Columbia Law Review*, 105, pp. 279-318, 2005. Disponível em: <https://ssrn.com/abstract=594101>.

KIST, Dário José. *Prova Digital no Processo Penal,* 2ª ed. rev., ampliada e atualizada. Leme: Mizuno, 2024.

LÉVY, Pierre. *O que é virtual?* Tradução Paulo Neves, 2ª Ed. São Paulo: Editora 34, 2011.

LIGUORI, Carlos. *Direito e Criptografia*: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia 1ª Ed. São Paulo: SaraivaJur, 2022.

LOPES JUNIOR, Aury. *Direito Processual Penal* - 21ª Edição. Rio de Janeiro: Saraiva, 2024.

LORDELO, João Paulo. *Constitucionalismo Digital e Devido Processo Legal*, 2ª ed. Revista e atualizada. São Paulo: JusPodivm, 2024.

MARAFIOTI, Luca. Prueba Digital y Proceso Penal. *Revista de Derecho Penal y Proceso Penal*, n. 11, nov./2012.

MASON, Stephen; SHELDON, Andrew; DRIES, Hein. Proof: The Technical collection and examination of electronic evidence. In: MASON, Stephen; SENG, Daniel. *Electronic Evidence and Electronic Signatures,* v. 5. Londres: University of London Press, 2021. Disponível em: <http://www.jstor.org/stable/j.ctv512x65.16>.

MENDES, Clarissa Braga. *Segurança Jurídica e Justiça das Decisões Judiciais em Matéria Constitucional*. Dissertação – Instituto de Direito Público (IDP), Brasília, 2014.

MENDES NETO, José Guimarães. *Provas penais na era digital* – Desafios constitucionais e legais para recolha de dados à revelia do portador. Prefácio de Gilmar Mendes. São Paulo: Marcial Pons, 2024.

MENEZES, Alfred J.; OORSCHOT, Paul C. van; VANSTONE, Scott A. *Handbook of Applied Cryptography*, 2nd ed. Boca Raton (FL-EUA): CRC Press, 1996.

MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. *Nota Técnica n. 4* – Documentação da Cadeia de Custódia. Secretaria Especial de Políticas Criminais,

Centro de Apoio Operacional Criminal – CAOCrim. São Paulo: MPSP, 2020. Disponível em: <https://biblioteca.mpsp.mp.br/PHL_img/PGJ/004-nt%202021.pdf>.

MISAGHI, Mehran. *Um Ambiente Criptográfico Baseado na Identidade*, Tese – Universidade de São Paulo (Escola Politécnica), São Paulo, 2008.

MURGIA, Severino. *Prova Informatica e Processo Penale*. Tese – Università Degli Studi di Pavia, Pavia, 2017.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Special Publication (SP) 800-86* Guide to Integrating Forensic Techniques into Incident Response, Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, Technology Administration. Gaithersburg: U.S. Department of Commerce, 2006.

NERES, Winícius Ferraz. A cadeia de custódia dos vestígios digitais sob a ótica da Lei n. 13.964/2019: aspectos teóricos e práticos. *Boletim Científico Escola Superior do Ministério Público da União*, n. 56, p. 338–382, 2021. Disponível em: <https://escola.mpu.mp.br/publicacoescientificas/index.php/boletim/article/view/603>.

OXFORD ENGLISH DICTIONARY, s.*v. Hash (n. 1) e (n. 3)*. Disponível em: <https://doi.org/10.1093/OED/6068424098>.

PATIL, Harsh; KOHLI, Ravshish Kaur; PURI, Sorabh; PURI, Pooja. Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework. *Egyptian Journal of Forensic Sciences*, v. 14, n. 1, p. 1-9, 2023. Disponível em: <https://doaj.org/article/655cc4415a854089a0e844bb4da6cf94>.

PILKINGTON, Marc. Blockchain Technology: Principles and Applications. In: OLLEROS, F. Xavier; ZHEGU, Majlinda. *Research Handbook on Digital Transformations*. Northampton (MA-EUA): Edward Elgar, 2016. Disponível em: <https://ssrn.com/abstract=2662660>.

PRADEEP, K. C.; SOMAN, Rajashree; HONNAVALLI, Prasad. Validity of Forensic Evidence Using *Hash* Function. In: *Proceedings of the Fifth International Conference on Communication and Electronics Systems* (ICCES 2020), IEEE Conference Record # 48766, 2020. Disponível em: <https://ieeexplore.ieee.org/document/9138061/>.

PRADO, Geraldo. *Prova Penal e Sistema de Controles Epistêmicos* – a quebra da cadeia de custódia das provas obtidas por métodos ocultos, 1ª ed. São Paulo: Marcial Pons, 2014.

PRESIDÊNCIA DA REPÚBLICA. *Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes*, Gabinete de Segurança

Institucional, 21/IN01/DSIC/GSIPR, 08 de outubro de 2014. Disponível em: <https://www.gov.br/gsi/pt-br/ssic/legislacao/NC21.pdf>.

RASJID, Zulfany Erlisa; SOEWITO, Benfano; WITJAKSONO, Gunawan; ABDURACHMAN, Edi. A review of collisions in cryptographic *hash* function used in digital forensic tools. *Procedia Computer Science*, v. 116, p. 381-392, 2017. Disponível em: <https://doi.org/10.1016/j.procs.2017.10.072>.

REIBER, Lee. *Mobile Forensic Investigations*: A Guide to Evidence Collection, Analysis and Presentation, 1a ed. McGraw Hill, 2015.

REIS, Paulo Victor Alfeo. *Algoritmos e o Direito*. São Paulo: Almedina, 2020.

RIBEIRO, Ivan Morais. *O controle penal das criptomoedas*. 1. ed. São Paulo: J.M. Bosch, 2022. Disponível em: <https://doi.org/10.2307/j.ctv2zp4scd>.

RIVEST, Ronald Linn. The MD4 Message Digest Algorithm. In: RFC 1320, abril de 1992. Boston: MIT and RSA Data Security Inc., 1992.

ROSA, Gerson Faustino; DUARTE, Myllena Gonçalves. Crimes de Colarinho Branco: uma análise crítica da seletividade do sistema penal e a incapacidade de enfrentamento das organizações criminosas. In: *Revista Eletrônica da Faculdade de Direito de Franca,* v.17, n. 2, 2023. Disponível em: <https://revista.direitofranca.br/index.php/refdf/article/view/1428>.

SECRETARIA DE SEGURANÇA PÚBLICA. *Ocorrências Policiais registradas por mês* – Criminal. São Paulo, 2024. Disponível em: <https://www.ssp.sp.gov.br/estatistica/dados-mensais>.

SILVA, Johan Matos Coelho da; SILVA, Philipe Matos Coelho da. *Técnicas de detecção e classificação de malwares baseada na visualização de binários*. Monografia – Universidade de Brasília, Brasília, 2018.

SILVA, Rafael Velasquez Saavedra da. Ferramentas Analíticas Aplicadas no Enfrentamento da Corrupção. In: JORGE, Higor Vinícius Nogueira (coord.). *Enfrentamento da Corrupção e Investigação Criminal Tecnológica* – Procedimentos, fontes abertas, estudos de casos e direito anticorrupção. Salvador: JusPodivm, 2020.

SOUZA, Lia Andrade de; VASCONCELLOS, Vinicius G. A cadeia de custódia da prova obtida por meio de interceptações telefônicas e telemáticas: meios de proteção e consequências da violação. *Revista da Faculdade de Direito UFPR, [S. l.]*, v. 65, n. 2, p. 31–48, 2020. DOI: 10.5380/rfdufpr.v65i2.68577..

STALLINGS, William. *Cryptography and Network Security* – principles and practice, 7th ed., global edition. London: Pearson, 2017.

SUPERIOR TRIBUNAL DE JUSTIÇA. *Boletim Estatístico – Novembro de 2024*. Brasília: STJ, 2024 Disponível em: <https://www.stj.jus.br/docs_internet/processo/boletim/2024/Boletim202411.pdf>, acesso em 03/01/2025.

TARUFFO, Michele. *A Prova*, trad. João Gabriel Couto, Filosofia e Direito. São Paulo: Marcial Pons, 2014.

TILBORG, Henk C.A. van; JAJODIA, Sushil (ed.). *Encyclopedia of Cryptography and Security*, 2a ed. New York: Springer, 2014

TRIBUNAL SUPERIOR ELEITORAL. *Glossário de TI*. Brasília: TSE, 2024. Disponível em: <https://www.tse.jus.br/comunicacao/glossario-de-ti>.

U.S. DEPARTMENT OF JUSTICE (FEDERAL BUREAU OF INVESTIGATION). *Regional Computer Forensics Laboratory Annual Report for Fiscal Year 2007*. Washington: U.S. Departament of Justice, 2007.

VERDELHO, Pedro. A obtenção de prova no ambiente digital. In: *Revista do Ministério Público de Lisboa*, Lisboa, v. 25, n. 99, p. 117-136, jul./set. 2004. Disponível em: <http://201.23.85.222/biblioteca/index.asp?codigo_sophia=49232>. Acesso em 21/10/2024.

WANG, Xiaoyun; YU, Hongbo. Collisions for *hash* functions MD4, MD5, HAVAL-128 and RIPEMD. In: *Proceedings of the Annual International Cryptology Conference* (CRYPTO), 2005. Disponível em: <https://www.semanticscholar.org>,;

WE ARE SOCIAL & MELTWATER, *Digital 2023 Global Overview Report*, 2023. Disponível em <https://datareportal.com/reports/digital-2023-global-overview-report>.

ZAIKIN, Oleg. Inverting cryptographic *hash* functions via cube-and-conquer. *Journal of Artificial Intelligence Research*, 81, 2024. Disponível em: <https://dl.acm.org/doi/pdf/10.1613/jair.1.15244>.

Authorship information

Yuri Fisberg. Doutorando da Faculdade de Direito da Universidade de São Paulo (Departamento de Processo – Penal). Mestre em Direito pela Universidade de São Paulo. Especialista pela Escola Paulista da Magistratura. Promotor de Justiça do Ministério Público do Estado de São Paulo. yfisberg@usp.br

Additional information and author's declarations (*scientific integrity*)

Conflict of interest declaration: the author confirms that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

Declaration of originality: the author assures that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; he also attests that there is no third party plagiarism or self-plagiarism.

Data Availability Statement: In compliance with open science policies, the dataset of this article is available in an open repository at the following link: https://doi.org/10.48331/scielodata.T2RHA3.

Editorial process dates (https://revista.ibraspp.com.br/RBDPP/about)

- Submission: 23/04/2025
- Desk review and plagiarism check: 03/07/2025
- Correction round return 1: 04/07/2025
- Review 1: 14/07/2025
- Review 2: 29/07/2025
- Review 3: 13/08/2025
- Preliminary editorial decision: 17/09/2025
- Correction round return 2: 20/09/2025
- Final editorial decision: 26/09/2025

Editorial team

- Editor-in-chief: 1 (VGV)
- Reviewers: 3

How to cite (ABNT Brazil):

FISBERG, Yuri. Função '*hash*' e a integridade da prova digital. *Revista Brasileira de Direito Processual Penal*, vol. 11, n. 3, e1227, set./dez. 2025. https://doi.org/10.22197/rbdpp.v11i3.1227