

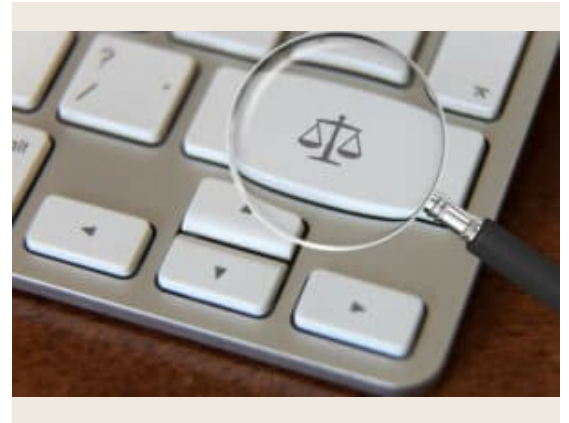
Validade da prova digital: autenticidade, integridade e cadeia de custódia na jurisprudência do STJ

17/07/2026

A digitalização das relações sociais, comerciais e criminosas mudou a forma de provar fatos em juízo. Conversas de aplicativos de mensagens, registros de geolocalização, contratos firmados por biometria facial e publicações em redes sociais aparecem, hoje, no centro de litígios cíveis e de persecuções penais. O problema é que a prova digital, justamente por ser tão frequente, também pode ser a mais vulnerável. Dados eletrônicos podem ser alterados, apagados ou fabricados com rapidez, baixo custo e, muitas vezes, sem marcas evidentes para quem analisa apenas uma captura de tela ou um arquivo isolado.

Essa tensão explica por que a jurisprudência passou a olhar para a prova digital a partir de três ideias centrais: autenticidade, integridade e cadeia de custódia.

Autenticidade é a possibilidade de vincular o registro ao seu verdadeiro autor. Integridade é a segurança de que o conteúdo permaneceu o mesmo desde a coleta até a apresentação em juízo. Cadeia de custódia é a documentação do caminho percorrido pelo vestígio, com indicação de quem o coletou, como foi preservado, quem teve acesso e de que forma chegou ao processo.



Esses requisitos não são meras expressões técnicas. Eles se comunicam. Sem uma cadeia minimamente documentada, a integridade fica difícil de demonstrar. Sem integridade, a autoria perde força. Afinal, pouco adianta afirmar quem teria produzido determinado conteúdo se não é possível assegurar que o conteúdo apresentado em juízo é o mesmo que existia na origem.

Enquadramento normativo

O Direito brasileiro ainda não possui um estatuto único da prova digital. No processo civil, a admissibilidade decorre da liberdade dos meios de prova prevista no artigo 369 do CPC. Essa regra é complementada por dispositivos específicos: o artigo 422, § 1º, trata das fotografias digitais e das extraídas da internet; os artigos 439 a 441 disciplinam o documento eletrônico; e o artigo 384, parágrafo único, admite que dados representados por imagem ou som, gravados em arquivos eletrônicos, constem de ata notarial. Também devem ser consideradas a MP 2.200-2/2001, relativa à ICP-Brasil, e a Lei 14.063/2020, que classifica as assinaturas eletrônicas em simples, avançadas e qualificadas.

Spacca

No processo penal, o ponto de partida está nos artigos 158-A a 158-F do CPP, introduzidos pela Lei 13.964/2019. A cadeia de custódia passou a ser definida como o conjunto de procedimentos destinado a manter e documentar a história cronológica do vestígio, permitindo rastrear sua posse e seu manuseio desde o reconhecimento até o descarte. Embora o CPP não detalhe um procedimento próprio para evidências digitais, o STJ tem utilizado a ABNT NBR ISO/IEC 27037:2013 como parâmetro técnico de análise, especialmente pelos atributos de auditabilidade, repetibilidade, reprodutibilidade e justificabilidade [1].

Nessa discussão, o código hash ganhou papel central. Trata-se de um identificador único gerado a partir do conteúdo de um arquivo. Na prática, funciona como uma impressão digital do dado eletrônico. Se o conteúdo for alterado, ainda que minimamente, o hash muda. Por isso, a comparação entre hashes calculados no momento da coleta e em etapa posterior é um dos caminhos mais seguros para demonstrar a integridade do material.



Processo penal: rigor técnico e análise do caso concreto

A jurisprudência criminal do STJ passou por fases bem perceptíveis. Um marco inicial foi o RHC 99.735/SC, no qual a 6ª Turma considerou inválida a prova obtida por espelhamento de conversas via WhatsApp Web. A razão foi objetiva: a ferramenta permite envio e exclusão de mensagens sem deixar vestígios claros no aplicativo ou no computador, o que compromete a confiabilidade do material produzido por esse meio [2].

O ponto de maior rigor veio com o HC 828.054/RN, julgado pela 5ª Turma em 2024. Naquele caso, policiais, de posse de celular apreendido ligado e desbloqueado, consultaram diretamente o aparelho e capturaram telas de conversas. Não houve extração por ferramenta adequada, cálculo de hash, documentação técnica das etapas nem laudo capaz de demonstrar a metodologia empregada. O STJ declarou a inadmissibilidade da prova digital, destacando que a falta de procedimentos para garantir a idoneidade e a integridade dos dados extraídos de celular apreendido resulta em quebra da cadeia de custódia [3].

Esse precedente é importante porque deixa clara uma premissa de controle da atividade estatal. No processo penal, não basta afirmar que a prova veio da autoridade pública. Cabe ao Estado demonstrar a integridade e a confiabilidade da fonte que pretende utilizar contra o acusado. A atuação estatal é objeto de controle de legalidade, não parâmetro suficiente para dispensá-lo.

A partir de 2025, contudo, a orientação passou a ser aplicada com maior atenção às particularidades do caso concreto. No Inquérito 1.658/DF, a Corte Especial assentou que, para reconhecer a ilicitude de prova obtida mediante print de WhatsApp, é indispensável comprovar



a efetiva quebra da cadeia de custódia.[4]. A premissa foi absorvida pelas turmas criminais em julgados posteriores: se não há demonstração de adulteração, alteração da ordem cronológica das conversas ou interferência concreta na prova, a nulidade não deve ser presumida.

Esse movimento não significa abandono do rigor técnico. Significa, antes, que a cadeia de custódia não pode ser transformada em fórmula automática de nulidade. A irregularidade precisa ser examinada em sua capacidade real de comprometer o contraditório e a confiabilidade da prova. Foi essa a lógica do HC 653.515/RJ, no qual o STJ afirmou que eventual quebra da cadeia de custódia deve ser sopesada com os demais elementos da instrução, deslocando a discussão, conforme o caso, para o plano da valoração probatória [5].

A distinção prática é relevante. Quando a coleta é feita pelo Estado, mediante apreensão de aparelho, extração de dados ou manipulação de arquivos digitais, o rigor metodológico deve ser elevado. Quando se trata de print apresentado por vítima ou particular, confirmado em juízo e sem indício concreto de manipulação, a tendência mais recente do STJ é admitir a prova, reservando a perícia para hipóteses de dúvida objetiva sobre autenticidade ou integridade [6].

A melhor síntese, portanto, não é dizer que print é sempre inválido, nem que print é sempre suficiente. O ponto decisivo é a confiabilidade demonstrável. A prova digital deve ser analisada a partir de sua origem, de seu modo de coleta, da preservação da fonte original, da possibilidade de conferência e da existência de impugnação específica.

Prova digital no processo civil

No processo civil, a dinâmica é diferente. Vigora o ônus da impugnação especificada, previsto no artigo 341 do CPC, e a distribuição probatória do artigo 373, com possibilidade de inversão no consumo e de redistribuição dinâmica em situações concretas. Em regra, o documento eletrônico não impugnado de forma adequada tende a ser admitido como elemento probatório. Quando há impugnação séria, surge a necessidade de demonstrar sua fidedignidade.

Embora a cadeia de custódia esteja positivada no CPP, sua lógica vem sendo utilizada no processo civil como critério racional de valoração. Quanto mais documentado, auditável e verificável for o percurso do dado, maior será sua força persuasiva. Quanto mais opaco for esse percurso, maior será sua vulnerabilidade à impugnação.

As capturas de tela de conversas são o exemplo mais comum. Isoladamente, prints são frágeis. Eles não revelam metadados, não permitem conferência da fonte original e podem ser editados com facilidade. A ata notarial, prevista no artigo 384 do CPC, continua sendo um instrumento relevante de robustecimento, pois documenta a existência e o modo de existir do conteúdo digital por meio de tabelião dotado de fé pública. Ao lado dela, ganham espaço plataformas de captura técnica que registram carimbo de tempo, hash e trilha de auditoria.

Em qualquer cenário, a boa prática é preservar a fonte original. Essa providência simples costuma ser decisiva. Se a prova for impugnada, a parte que preservou o aparelho, o arquivo original, os logs ou a base de dados terá melhores condições de sustentar a autenticidade e a integridade do material.

Contratação eletrônica, biometria e responsabilidade do fornecedor

A contratação eletrônica também se tornou campo fértil de discussão, especialmente em operações bancárias e de crédito consignado. O STJ reconhece a eficácia da contratação eletrônica e já admitiu, em situação específica, a executividade de contrato eletrônico assinado digitalmente mesmo sem a subscrição de duas testemunhas [7]. Mais recentemente, a corte reforçou que a falta de credenciamento da certificadora na ICP-Brasil, por si só, não invalida a assinatura eletrônica quando existirem outros elementos confiáveis de autenticação [8].

Isso não significa, porém, que todo contrato eletrônico seja automaticamente válido. A validade da biometria facial depende da qualidade do dossiê de contratação. Logs de acesso, geolocalização, IP, prova de vida, trilha de auditoria, identificação do dispositivo, hash dos documentos e preservação dos arquivos originais podem ser decisivos. Sem esses elementos, a instituição financeira tende a suportar o ônus da fragilidade probatória, sobretudo quando o consumidor impugna a autenticidade do contrato.

Essa conclusão dialoga diretamente com a Súmula 479 do STJ, segundo a qual as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Assim, quando o consumidor nega a contratação e impugna a autenticidade do vínculo, não basta apresentar telas internas ou documentos sem auditabilidade. É necessário demonstrar a trilha da contratação, e não apenas o seu resultado aparente [9].

Conclusão: regime de ônus recíprocos

A comparação entre processo penal e processo civil revela uma aproximação de critérios, mas com intensidades diferentes. No processo penal, em razão do standard probatório mais rigoroso e do controle da atividade estatal, a prova digital exige maior cuidado técnico. A falta de documentação mínima pode levar à inadmissibilidade, sobretudo quando inviabiliza o contraditório ou impede a verificação da integridade do dado.

No processo civil, a fragilidade técnica raramente exclui a prova de imediato. Em geral, ela reduz sua força persuasiva. Mas essa redução pode decidir o caso, principalmente quando a parte que tinha melhores condições de produzir um dossiê técnico opta por apresentar apenas telas, prints ou registros internos sem auditabilidade.

O ponto de equilíbrio que se desenha na jurisprudência é adequado. De um lado, rejeita-se a ideia de que qualquer falha formal na cadeia de custódia gere nulidade automática. De outro, também se rejeita a ingenuidade de presumir íntegro aquilo que é tecnicamente manipulável. Quem produz a prova digital deve municiá-la de rastreabilidade. Quem a impugna deve apontar o vício específico e o prejuízo concreto. Entre a formalização vazia e a credulidade tecnológica, os tribunais têm caminhado para um critério mais seguro: a confiabilidade demonstrável.

Notas



1. STJ, AgRg no HC 828.054/RN, 5ª Turma, rel. min. Joel Ilan Paciornik, j. 23.4.2024, DJe 29.4.2024, com referência à ABNT NBR ISO/IEC 27037:2013.
2. STJ, RHC 99.735/SC, 6ª Turma, rel. min. Laurita Vaz, j. 27.11.2018, DJe 12.12.2018.
3. STJ, AgRg no HC 828.054/RN, 5ª Turma, rel. min. Joel Ilan Paciornik, j. 23.4.2024, DJe 29.4.2024.
4. STJ, Inq 1.658/DF, Corte Especial, rel. min. Og Fernandes, j. 19.2.2025, DJEN 11.3.2025.
5. STJ, HC 653.515/RJ, 6ª Turma, rel. para acórdão min. Rogerio Schietti Cruz.
6. Entre outros: STJ, RHC 218.499/SC, 6ª Turma; AgRg no AREsp 2.600.503/ES, 6ª Turma; AgRg no AREsp 2.833.422/RS, 6ª Turma; AgRg no AREsp 2.841.690/SP, 5ª Turma.
7. STJ, REsp 1.495.920/DF, 3ª Turma, rel. min. Paulo de Tarso Sanseverino, j. 15.5.2018, DJe 7.6.2018.
8. STJ, REsp 2.159.442/PR, 3ª Turma, rel. min. Nancy Andrighi, j. 24.9.2024, DJe 27.9.2024; STJ, notícia institucional de 3.12.2024.
9. STJ, Súmula 479.

Fonte: <https://conjur.jumps.com.br/2026-jul-17/validade-da-prova-digital-autenticidade-integridade-e-cadeia-de-custodia-na-jurisprudencia-do-stj/>