Prova digital foi em 2025 e será em 2026 o grande tema do processo penal

26/12/2025

Se você não estava isolado do mundo nos últimos dois anos [*num retiro sabático*], então deve ter percebido, ainda que sem entender muito bem [*assim como eu*] a dimensão, nem o impacto, da *transformação digital* do mundo e, por consequência, no processo penal, com a inclusão de novos artefatos digitais que alteraram significativamente o modo como os humanos se relacionam, conhecem, pensam e decidem. Por isso, a compreensão adequada do processo criminal no contexto atual demanda a reconfiguração de diversas coordenadas analógicas que serviram de suporte à produção e à aplicação do aparato normativo e às práticas processuais orientadas ao mundo analógico, atualmente insuficientes, porque atravessadas pela digitalização, a avalanche de dados e informações, das provas digitais e da inteligência artificial [*geral e generativa*].

Spacca

Não abordarei a inteligência artificial porque mesmo quem critica usa, ainda que, em geral, não saiba usar, porque as oportunidades são imensas e, quem usa de modo adequado, por ser uma vantagem competitiva, não conta para quem usa inteligência artificial generativa como se fosse Google, nem quer pagar assinatura da versão pro, correndo o risco concreto de incorrer em um grande mico digital. Aliás, a primeira vez que escrevi aqui nesta **ConJur** sobre IA foi há quase oaito anos, em 2018 – Inteligência Artificial chegou chegando, seguida de diversos textos Ensinando um robô a julgar em 2020, IAGen na análise de prova penal, desafios de lidar com nato digitais, a ingenuidade do Aprendiz de feiticeiro digital, além dos micos de quem usa jurisprudência *fake*, colocando em risco a reputação: *ChatGPT*: 'Primeiro você alucina, inventa jurisprudência' ou 'não era julgado, era cilada'.

No entanto, o tema de hoje é prova digital ou evidência digital, como preferem os peritos. Se você atuou em processos penais em 2025 deve ter constatado que a quebra do sigilo de dados em dispositivos, artefatos e nuvem foi a principal prova produzida durante as investigações e, depois, utilizadas no como meio de prova para sustentar acusações e condenações. Por não terem sido ensinados sobre prova digital, em geral, os agentes processuais [*investigadores, acusadores, defensores e julgadores*], embora fazendo 'pose' de que entendem o que se passa, no fundo, pouco ou nada compreendem, deixando passar em branco grandes oportunidades digitais [quebra da cadeia de custódia; nulidades; desconformidades; manipulações; ausência de dados brutos, bilhetagem etc.] ou cometendo erros primários [alegar sem conhecer

minimamente ‘sobre’ o que fala, achando que dizer que a cadeia de custódia digital está quebrada, sem dizer onde e por qual motivo resolve], especialmente no caso de acusados defendidos por profissionais analógicos, alheios ao impacto tecnológico no processo penal.

Se o processo é eletrônico, a prova é digital e o defensor analógico, fomenta-se a ausência de defesa digital efetiva. É verdade que nem sempre o defensor dispõe de ferramentas, softwares e aplicativos necessários à atividade de reação técnica, embora hoje em dia já estejam disponíveis várias ferramentas *open-source* e, também, proprietárias de baixo custo, em regra, desconhecidas por quem está sentado à espera de um milagre digital [se não procurar no lugar certo, continuará reclamando nas redes sociais, talvez no *Facebook*, como bom ‘cringe’]. Para instauração do contraditório digital, a defesa deve saber do que se trata, incluindo aspectos técnicos suficientes ao exercício do contraditório efetivo.

No que interessa, a perícia digital se relaciona com o fenômeno criminal em que sistemas computacionais, *softwares* e aplicativos são empregados, em geral, de 3 modos distintos: **[a]** Como **objeto** de um crime [p.ex: invasão de dispositivo informático]; **[b]** Como **instrumento** para cometer um crime [*p.ex: estelionato eletrônico; fraudes digitais etc.*]; ou, **[c]** Como **repositório de evidências** relacionadas a um crime.

O termo “evidência digital” é preferido no campo técnico, em contraste com o de “prova digital”, por se referir aos dados brutos em formato binário [*bit*], exigindo a aquisição, recuperação e análise. A distinção principal situa-se na atividade técnica subjacente em relação aos dados e metadados em si, nas metodologias e nos procedimentos aplicados, com foco na integridade e autenticidade do dado em formato binário.

Segundo a ISSO 27037, são 4 (quatro) os atributos-chave à rastreabilidade e garantia da integridade e a validade das evidências em qualquer contexto investigativo ou processual, já ensinava Geraldo Prado, o precursor da importância da cadeia de custódia no Brasil: **[a] auditabilidade:** É a capacidade de rastrear e documentar cada passo do processo de manuseio das evidências digitais (desde a identificação, coleta, armazenamento, transferência e uso).

A auditabilidade garante que as evidências sejam manuseadas de maneira que preserve a integridade e a autenticidade, condição de admissibilidade; **[b] justificabilidade:** Refere-se à necessidade de explicar e fundamentar todas as decisões tomadas durante o manuseio das evidências, implicando na demonstração do ‘*por que*’ determinadas evidências foram coletadas e ‘*como*’ foram coletadas, garantindo-se a transparência; **[c] repetibilidade:** É assegurada quando resultados **consistentes** de testes são obtidos sob condições específicas, como a aplicação de procedimentos e métodos de análise idênticos, usando equipamentos semelhantes [obtenção dos mesmos resultados aplicados idênticos procedimentos]; e, **[d] reprodutibilidade:** É confirmada quando resultados idênticos de testes são obtidos sob circunstâncias variadas, utilizando métodos de avaliação semelhantes, mas com equipamentos distintos e em condições diversas. A reprodutibilidade do processo é um critério relevante à admissibilidade do meio de prova [o que não pode ser reproduzido deve ser rejeitado].

Por outro lado, a admissibilidade de qualquer prova digital em um processo judicial depende da possibilidade de verificação da integridade e autenticidade. A **integridade** é a característica de

um dado que permite detectar qualquer alteração de conteúdo eventualmente realizada, associada à condição de que os dados estejam **completos, intactos e não modificados** desde o momento da coleta, preservando-se a integridade conforme a ISO 27037, admitida expressamente no julgamento relatado pelo ministro Joel Ilan Paciornik em setembro de 2025 (**HC 1.036.370**). A falha em aderir a procedimentos documentados pode comprometer a validade e o uso das evidências digitais em investigações ou procedimentos legais.

A **autenticidade** garante que a prova foi coletada em sua integralidade e sem qualquer modificação, contaminação ou parcialidade, permitindo a repetição de todos os procedimentos feitos pelos peritos oficiais. O princípio fundamental que orienta um exame forense sólido é que a evidência original não deve ser alterada de forma alguma. Por isso, o exame forense deve ser realizado em uma cópia fiel da evidência, a ser fornecido na integralidade à defesa [dados brutos].

A **integridade** dos dados é verificada pelo algoritmo/função de *hash*, que funciona como uma "impressão digital" digital do dado. Definição: O *hash* é um algoritmo matemático que gera, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo (condensação). Validação: Se um único *bit* da entrada for alterado, acrescentado ou retirado, o *hash* se altera completamente. Aplicação: O cálculo dos *hashes* [SHA-256, recomendado nos POPs do Ministério da Justiça; SHA-512, desde que seguros: confira aqui] é essencial na fase de aquisição e preservação para: **[a]** garantir a integridade dos dados coletados, confirmando que não foram alterados ou corrompidos; e, **[b]** assegurar a autenticidade dos dados adquiridos, fortalecendo a base de conformidade. Nota prática: Para que a evidência seja admissível, deve haver um método científico para validar que a evidência apresentada (a cópia) é exatamente a mesma que a originalmente coletada. O *hash* fornece este registro auditável que prova em tribunal que as evidências são autênticas. O *hash* dos arquivos extraídos deve constar no documento produzido pelo perito e no termo de apreensão.

Os pontos destacados apresentam um panorama geral da prova digital, servindo de ponto de partida. Em 2025 aprendi muito com conversas online com peritos e profissionais que com paciência e hospitalidade, procuram ensinar e aprender, dentre os quais agradeço: Leandro Morales Baier Stefano, Daniel Ávilla, Lorenzo Parodi, Antônio Souza, Joaquim Bartolomeu Ferreira Neto, Dellano Sousa, Bárbara Guasque, Flaviane Bolzan de Morais, Gustavo Rabay, Gabriel Bulhões, Alesandro Gonçalves Barreto, Emerson Wendt, Romullo Carvalho, Denis Sampaio, Sheyner Ásfora, Flávio Pansieri, Thiago Minagé, Adriana Spengler, Rui Cunha Martins, Marco Marrafon, Rubens Pavarin, Alexandre Simas Santos, Cauã Dacol, André Dacol, Tamyres Xavier, Edward Carvalho, Ellestron Canali e Vítor Paczek, além dos parceiros de coluna Aury Lopes Jr. e Jacinto Nelson de Miranda Coutinho.

Agradecemos, em nome dos colunistas, ao diretor de Redação, Márcio Chaer, pela acolhida, ao time da **ConJur**, em especial ao parceiro de todas as horas, o editor de Opinião, Emerson Voltare. Escrevo na revista eletrônica **Consultor Jurídico** desde 2013, lá se vão mais de 12 anos. Obrigado.

Boas Festas e que venha 2026!

De presente, segue uma lista de artigos curtos que podem auxiliar na aprendizagem contínua sobre o mundo digital:

Prova penal digital: relatórios do *Cellebrite* podem ser insuficientes?

Como recuperar ou apagar dados em dispositivos? Riscos da prova digital

STJ anula condenação por ausência de integralidade da prova digital

Colisão de MD5 e SHA-1 em vestígios digitais: risco real para integridade da prova

Prova penal digital: relatórios do *Cellebrite* podem ser insuficientes?

Prova digital comprometida pela simples alteração da data no dispositivo apreendido

Vulnerabilidades nos arquivos UFDR da Cellebrite: impactos e riscos da cadeia de custódia

O fim do cabo USB no iPhone. Perícia somente em nuvem

Recuperação de mensagens apagadas em smartphones: mitos, realidades e recomendações

Como criar 'prints' falsos: quando as aparências enganam e a cadeia de custódia dos vestígios digitais

Como usam sua selfie para abrir contas por meio do reconhecimento facial

A responsabilidade pelo 'sequestro' de contas do Instagram por meio de *SIMswap*

Textos de Lorenzo Parodi na ConJur

Ferramentas de Osint: Wigle.net — geolocalização, privacidade e prova digital

Alexandre Morais da Rosa – Roteiro de Aprendizagem

SkyECC e os desafios probatórios no processo penal

Fonte: https://conjur.jumps.com.br/2025-dez-26/prova-digital-foi-em-2025-e-sera-em-2026-o-grande-tema-do-processo-penal/