# Prova digital: duplicação forense como standard de admissibilidade

06/12/2024

Ao longo dos anos os tribunais superiores foram construindo critérios decisórios importantes sobre as provas derivadas de suportes informáticos, impondo o desentranhamento (inadmissão) quando:

> – *for identificada a busca randômica de dados (HC 315220);*
> – *não houver disponibilização dos dados originais e íntegros (REsp 179534);*
> – *em situações de prints screens de whatsapp que são facilmente sujeitos às interferências externas (AgRg no AREsp 2441511 e AgRg no RHC 133.430);*
> – *extrações de conversas de aplicativos feitas "artesanalmente", sem softwares convencionais com método certificado (AgRg no HC n. 828.054);*

São teses com rigor científico que corretamente são acolhidas pelo STJ, mas que estão em constante tensão sobre o desacerto das conclusões, havendo julgamentos antagônicos dentro do sistema de justiça. Contudo, recentemente foi fixado nos Tribunais Superiores um relevante entendimento a respeito das provas digitais: **a inadmissibilidade da prova pela inexistência de duplicação forense**.

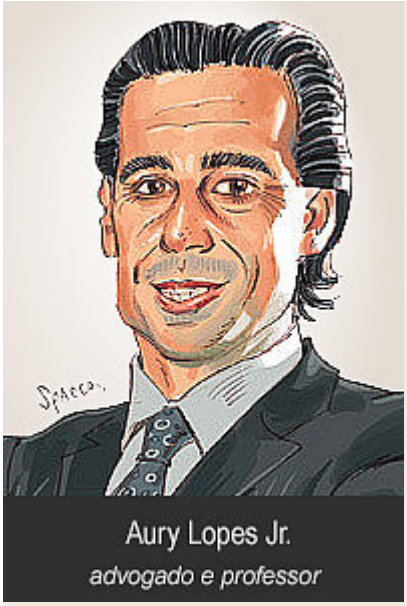
Na literatura forense, se existe um consenso científico a respeito de determinado assunto **é de que a quebra da cadeia de custódia das provas digitais leva, sem exceção, à inadmissibilidade da prova** [1]**,** devido ao método científico específico que impede valorações mitigadas, exatamente por que no campo da computação forense, as provas sem autenticidade e integridade não possuem conteúdo verdadeiro.

As práticas de adulteração culposa — como a realização de múltiplas cópias sem controle, obtenção de *backups* incompletos, manuseios dos dados sem bloqueio de conteúdo — convivem com as práticas *anti-forense* e com as coletas feitas por *bigtechs* sem metodologia forense adequada. Esse conjunto de problemas no tratamento das provas digitais torna as modificações nos dados normalmente indetectáveis, o que suprime o parâmetro de controle entre prova adulterada *vs* íntegra.

## Volatilidade

É a partir da perspectiva de volatilidade do dado digital que se deve pensar a duplicação (cópia) forense como o primeiro e mais importante ato da cadeia de custódia das provas digitais**, que é tecnicamente chamado de *image*, cópia *bitstream*** ou *bit* a *bit* [2].

*Spacca*




Somente com ele vamos ter uma cópia fiel, idêntica, atingindo o equivalente à originalidade do vestígio digital capturado. Ela precisa ser feita por um Perito (e não por um policial, ainda que possua conhecimento sobre tecnologias forenses; mesma lógica do juiz de garantias), que deve gerar uma *image*, equivalente a uma fotografia digital, uma cópia mestra protegida e idêntica, normalmente elaborado por meio do software FTK *Imager* em ambiente controlado. Criada a *image*, é preciso protegê-la de alterações, confirmar sua integridade e validar sua autenticidade, o que normalmente é feito por aposição de *hash* [3],que equivale a uma *impressão digital*[4]¯[5].

A partir daqui, somente a cópia forense vai ser entregue para os investigadores analistas trabalharem, preservando-se os vestígios originais em centrais de custódia, para cumprir o dever de integridade.

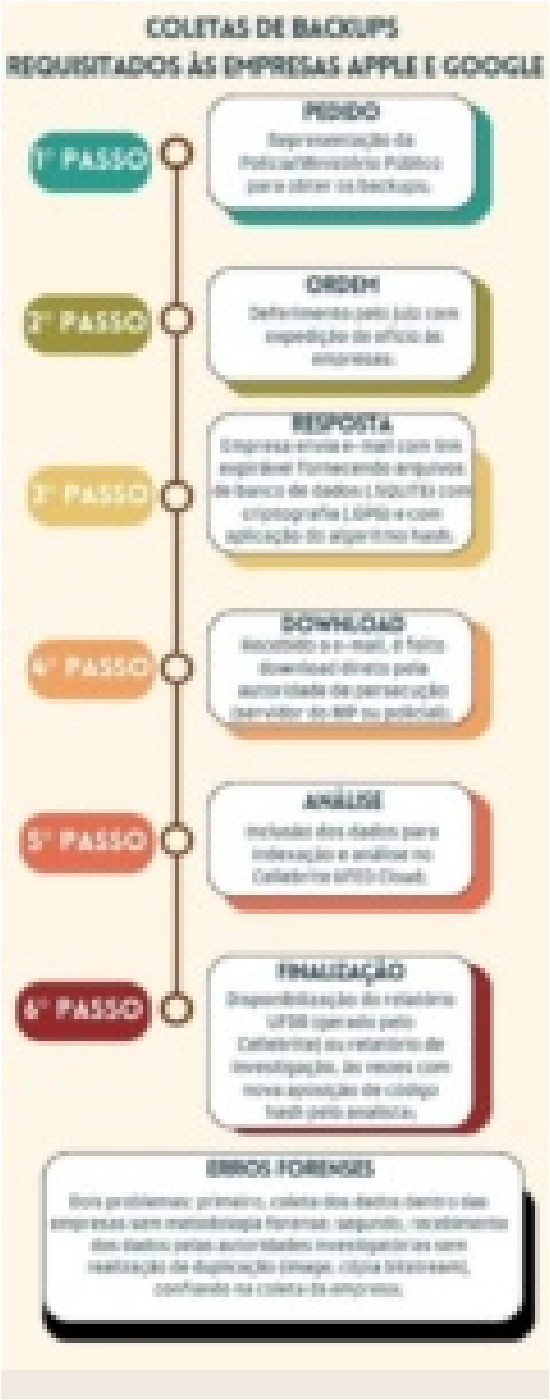
Nos tribunais superiores, há ao menos 4 precedentes importantes sobre a essencialidade da duplicação forense, tratando-se de *standard* de admissibilidade da prova digital, que se descumprido leva à exclusão da prova: STJ, AgRg no RHC nº 143.169, Rel. para o acórdão Min. Ribeiro Dantas, 5ª Turma, 07/02/23; RHC 188.154, Rel. Ministra Daniela Teixeira, 22/07/24; AgRg no HC 828054, Rel. Min. Joel Ilan Paciornik, 5ª Turma, 23/04/24; STF, 2º AgRg no ARE nº 1.343.875, Rel. Min. Ricardo Lewandowski, 2ª Turma, 08/08/22.

Cita-se como exemplo a parte mais importante do último julgado, entre os 4 acima mencionados:

> *"(...) para que se faça a extração de provas digitais de uma mídia é preciso realizar a cópia ou espelhamento do suporte em que está registrado o arquivo de dados, o que normalmente se faz com o chamado código hash (...) Dou provimento ao recurso em habeas corpus para reconhecer a violação da cadeia de custódia da prova digital (...) ".(Dec. Mon. Ministra Daniela Teixeira no RHC n. 188.154, DJe de 24/07/2024).*

Contudo, em diversas investigações criminais brasileiras, a coleta dos *backups* armazenados em nuvem tem sido feita pelas autoridades de persecução da seguinte forma:

*Reprodução*




Esse caminho do vestígio é uma situação exemplar em que não houve a instauração da cadeia de custódia logo no momento da identificação e coleta do vestígio, tratando-se de situação mais grave que a quebra: estamos diante de um cenário de completa inexistência de cadeia de custódia, que torna inútil posterior revisão procedimental com o objetivo de documentar a custódia do vestígio.

O envio pelas empresas de arquivos criptografados só impede que quem não tenha a senha faça o acesso, ou seja, não garante a integridade do dado digital coletado. A aposição de *hash* pela empresa também é irrelevante, pois não há parâmetro de comparação para controle, exatamente por que não existe uma cópia originária para comparação; só se envia um único arquivo. As empresas não dispõem de metodologia forense adequada e não devem mesmo dispor, pois isso é atribuição dos peritos.

Embora os quatro julgamentos paradigmas sobre a duplicação forense lidem com dispositivos físicos (celulares, computadores, HDs etc), o raciocínio decisório é integralmente aplicável ao tratamento dos dados digitais armazenados em *nuvens*: a cópia forense deve ocorrer antes do analista policial trabalhar nos vestígios.

A rigor, no exemplo não se pode sequer falar em vestígio, que pressupõe um sentido de originalidade, tratando-se de prova que sequer deveria ter sido admitida, e se já admitida, imediatamente desentranhada dos autos. O processo penal brasileiro é débil em termos de controle de admissibilidade das provas, e por isso deve-se promover um momento anterior, de manifestação das partes, à decisão de admissibilidade pelo juiz [6].

Apesar da *fonte de prova digital* original permanecer sob o domínio do provedor (*bigtech*), possibilitar-se-á às partes processuais o conhecimento acerca de toda a metodologia utilizada, permitindo-se — portanto — a *rastreabilidade da fonte de prova digital* [7]coletada em *sistema de nuvens,* que é um dos conhecimentos mais relevantes (como se fez a coleta?) quando se trata da eficácia do contraditório das provas digitais.

O foco da discussão passa a ser sobre a qualidade do contraditório, em que somente será admissível uma *fonte* de prova digital no processo se comprovada a fiabilidade a partir da garantia da informação e reação (confronto) sobre os critérios adequados de recolha,

preservação e análise dos dados digitais. Um posterior contraditório será também efetivado no campo da valoração, voltado ao debate do conteúdo informacional trazido ao processo pela *fonte* probatória recolhida, que nesta oportunidade já admitida como *fonte* de prova lícita.

_____

[1] PARODI, Lorenzo. **Perícia defensiva em provas digitais no processo penal**. 1ª ed. São Paulo: RT, 2024; COSIC, Jasmin; COSIC, Zoran. Chain of custody and life cycle of digital evidence. **Computer Technology and Application 3** (2012) 126-129.

[2] Em nota técnica publicada pela Cloud Security Alliance, nome Mapping the Forensic Standard ISO/IEC 27037, a fase crucial da forense digital na computação em nuvem está na aquisição das provas, isto é, no processo de criação da cópia idêntica dos dados selecionados que na computação em nuvem, quando não se tem acesso ao dispositivo informático físico (por exemplo, celular), deve ocorrer através de acesso remoto que permitiria a captura em tempo real (*live forensics*), por meio de máquinas virtuais e capturas instantâneas (*snapshot* e *virtual machines introspector*). (**Incident Management and Forensics Working Group. Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing.** Disponível em: < https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf >)

[3] Cálculo matemático que gera um valor numérico baseado no *input* de dados. Este valor numérico é referido como valor de *hash*. (COSIC, Jasmin; BACA, Miroslav. *(***Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp**. 1226 – 1230. 10.13140/RG.2.1.1336.0725. 2010. p, 2. Disponível em: https://www.researchgate.net/publication/224163003_Improving_chain_of_custody_and_digital_evider

[4] RAMALHO, David. **Métodos ocultos de investigação criminal no ambiente digital**. p, 124. “Os algoritmos mais utilizados atualmente são o MD5 (*Message Digest 5*) e o SHA-1 ( *Secure Hash Algorithm*)”.

[5] Discorre Giuliano Giova (**Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems**. p, 3) que alguns *softwares* forenses modernos além de descreverem onde cada arquivo está localizado e suas muitas propriedades, incluindo data de criação e datas de acesso, permitem a criação de chaves específicas de acesso a usuários. Adotam o conceito de autenticação central e permissão de concessão a servidores que concedem tais chaves de sessão para usuários autorizados, monitorando desta forma toda a atividade de exame da cadeia de custódia da prova digital.

[6] MENDES, Carlos Hélder C. Furtado. **Prova Penal Digital***:* direito à não autoincriminação e contraditório na extração de dados armazenados em dispositivos informáticos. 1ª ed. São Paulo: Tirant lo Blanch, 2024.

[7] Ibidem.

Fonte: https://conjur.jumps.com.br/2024-dez-06/prova-digital-duplicacao-forense-como-standard-de-admissibilidade/