Prova digital comprometida pela simples alteração da data no dispositivo apreendido

22/08/2025

1. Questão

Este curto texto aborda a questão de como a simples alteração de data em smartphones pode comprometer irreversivelmente a validade das provas digitais.

2. Da prova analógica à prova digital-eletrônica

A revolução tecnológica transformou o regime de provas no processo penal. Enquanto o modelo analógico de provas físicas/tangíveis preserva, em geral, os atributos originais ao longo do tempo (arma, faca, instrumentos), a prova digital-eletrônica é intangível e depende da integridade e autenticidade das referências temporais constantes nos metadados, nem sempre coletados em conformidade com as normas técnicas e, pior, subtraídos do escrutínio defensivo, quando não fornecidos os dados brutos.

Sem o fornecimento da totalidade dos dados brutos, ainda que sejam possíveis manipulações de má-fé no intermédio entre a apreensão e a entrega ao perito, compromete-se o exercício da ampla defesa digital.

Por isso, a questão central a ser debatida é o da vulnerabilidade temporal dos dispositivos móveis quando submetidos à análise forense. Todo sistema computacional opera a partir de uma cronologia interna. Quando a referência temporal é alterada, por falha, necessidade técnica ou manipulação, todo o ecossistema digital do dispositivo passa a operar em uma nova linha temporal, impedindo a atribuição de confiabilidade histórica dos dados, ainda que aparentemente completos. O risco agrava-se para quem sequer conhece a estrutura, os tipos e as formas de armazenamento de dados em smartphones, comprando gato por lebre.

3. Vulnerabilidade temporal dos smartphones

Ao contrário de adulterações físicas, visíveis e detectáveis com pouco conhecimento técnico, as alterações de data em sistemas digitais são quase imperceptíveis em uma análise superficial. As inconsistências só aparecem em extrações completas, com acesso a logs de sistema e bancos de dados de aplicativos. Dito diretamente, quem quiser manipular o conteúdo de um smartphone de má-fé, consegue fazê-lo, sem ser detectado, porque estrategicamente omite o conteúdo que permitiria a detecção por um perito tecnicamente habilitado. O pior, conta com o assentimento alienado de parcela dos operadores do Direito que, muitas vezes, desconhecendo a estrutura da prova digital, acredita ingenuamente ser suficiente relatórios que entregam somente o que se deixa ver. É preciso deixar de ser trouxa digital.

Sem a extração integral disponibilizada à defesa, torna-se praticamente impossível identificar manipulações, abrindo-se espaço para falsas cronologias, capazes de induzir os agentes públicos de acusação e de julgamento em supostos fatos inexistentes, mas com aparência de verdade.

4. Efeito cascata das alterações

Os smartphones modernos operam com múltiplas camadas interconectadas: sistema operacional, aplicativos, metadados e bancos de dados. Todos dependem de sincronização temporal precisa, com registros internos, especialmente no banco de dados do aparelho/dispositivo.

Assim, a simples alteração da data gera um **efeito cascata**: aplicativos passam a registrar atividades com base na nova cronologia, documentos são gravados ou inseridos com timestamps (carimbo de tempo) falsos e sistemas de geolocalização podem indicar movimentações inexistentes.

Exemplo: se um celular apreendido em 15 de março tem sua data alterada para 10 de março, qualquer atividade posterior, inclusive atualizações automáticas ou registros de laboratório, será registrada como se tivesse ocorrido antes da apreensão. Tente fazer no seu smartphone: altere a data nas configurações e tire uma foto. Em seguida confira a data. Pasme excelência, será a alterada.

A implicação não é só para defesa. Considere que um acusado de má-fé antes ou depois de praticar um crime decide alterar a data do smartphone para criar um álibi falso, tirando fotos ou realizando ações com o smartphone para “comprovar” uma situação inventada, servindo de suporto álibi. Se a defesa deixar de fornecer a integridade dos dados, a acusação não poderá verificar a integridade, a confiabilidade e a validade do álibi fake.

Então, com absoluta razão, a defesa deve fornecer a integridade dos dados para perícia oficial. A mesma lógica aplica-se à acusação. Em resumo: prova digital eletrônica sem extração integral dos dados e submissão à análise da parte adversa é uma vulnerabilidade intolerável ao devido processo legal digital. O fair trial depende de prova lícita e auditável em sua integridade, sob pena de comportamentos oportunistas, tanto da acusação e da defesa. A lógica pode ser uma aliada.

5. Inconsistência lógica como prova

Um dos pontos mais reveladores são os **metadados**. É impossível, por exemplo, que o banco de dados do WhatsApp apresente data de última modificação em 27 de julho, mas contenha mensagens datadas de 5 de agosto. A incongruência é evidência científica inequívoca de manipulação temporal.

Outro exemplo: registros de GPS podem indicar a localização do laboratório forense em datas em que, teoricamente, o aparelho ainda estaria em posse do usuário.

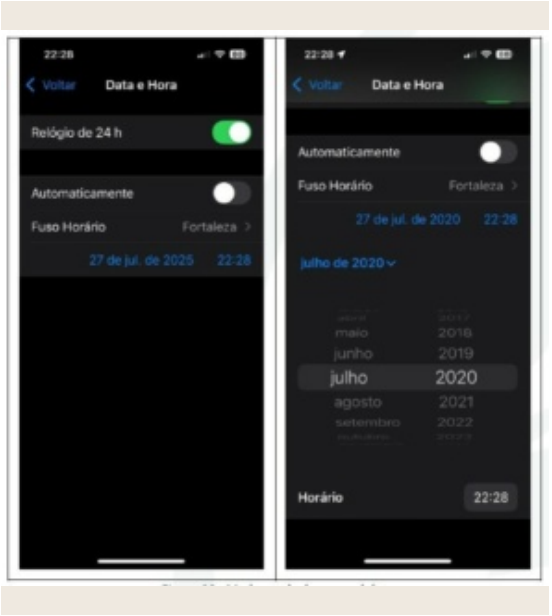
Os exemplos demonstram a inconsistência lógica.

6. Prova de conceito: o impacto prático da manipulação temporal

Para evidenciar, de forma científica, os riscos da alteração de data em dispositivos apreendidos, foi realizada uma **prova de conceito** utilizando um **iPhone 13**. A metodologia, embora aplicada a este aparelho, pode ser replicada em outros dispositivos móveis.

No **dia 27 de julho de 2025**, a data do aparelho foi propositalmente alterada para **27 de julho de 2020**. Em seguida, foi realizado registro fotográfico do site da **Hora Legal Brasileira (HLB – DISHO)**, que apresenta a data e hora oficiais na internet.

Após a captura da imagem, procedeu-se à análise dos metadados da fotografia. Constatou-se que, embora a foto não tivesse sido manipulada, as informações de data refletiam **exatamente a data alterada no sistema do celular** e não a data real do registro.



Essa simples prova de conceito demonstra, de maneira inequívoca, como a manipulação temporal compromete a confiabilidade das evidências digitais. Em processos judiciais, a consequência é grave: qualquer alteração, inserção ou exclusão de dados feita após a apreensão pode ser registrada como se tivesse ocorrido em período anterior, quando o celular ainda estava em posse do investigado.

Ou seja, mesmo sem adulterar diretamente o conteúdo, a referência temporal (atributo essencial da cadeia de custódia digital) — é corrompida, tornando o vestígio inutilizável do ponto de vista da confiabilidade científica.

7. Normas internacionais e melhores práticas

A comunidade científica já reconhece a gravidade dessa questão. O **ISO/IEC 27.037:2012** estabelece diretrizes claras para identificação, coleta e preservação de evidências digitais, com ênfase na manutenção da integridade temporal. O **RFC 3.227** reforça essas diretrizes, detalhando metodologias de preservação cronológica.

As melhores práticas incluem:

- isolamento imediato do dispositivo (modo avião e bloqueadores de sinal);
- documentação da data e hora do sistema no momento da coleta;
- criação de imagem forense completa antes de qualquer manipulação;
- registro detalhado de todos os procedimentos periciais.

8. Consequências processuais

As inconsistências temporais não são meros detalhes técnicos: comprometem diretamente os princípios da ciência forense — **reprodutibilidade, confiabilidade e validade**. Se a cronologia dos eventos não pode ser estabelecida com certeza científica, perde-se a capacidade de distinguir entre dados originais e dados gerados na própria análise.

No processo penal, isso significa colocar em risco a própria **admissibilidade da prova**, uma vez que a quebra da cadeia de custódia temporal fragiliza o valor probatório.

9. Caminhos para enfrentar o problema

Superar essa fragilidade exige uma abordagem multifacetada:

- aprimoramento de protocolos técnicos;
- capacitação contínua de peritos e operadores do Direito;
- desenvolvimento de ferramentas capazes de detectar manipulações temporais;
- auditorias rigorosas nos procedimentos periciais.

Mais importante: é necessário reconhecer que a ciência forense digital é uma área em constante evolução, exigindo atualização permanente de métodos e procedimentos.

10. Breve conclusão

A era digital trouxe possibilidades extraordinárias para a investigação criminal, mas também novos riscos. A manipulação temporal de dispositivos apreendidos é um perigo oculto que pode corromper irreversivelmente a validade das evidências digitais.

Não se trata de desestimular o uso de provas digitais, algo irreversível. A exigência é de tratamento rigoroso e cientificamente fundamentado. A preservação da integridade temporal é responsabilidade compartilhada de todos os agentes do sistema judicial.

Somente com colaboração interdisciplinar e compromisso com a excelência técnica será possível garantir que as evidências digitais cumpram sua função democrática: punir culpados e exonerar inocentes, evitando-se erros (falsos positivos ou falsos negativos). Para isso, entretanto, além de alfabetização e letramento digital, mostra-se necessário superar equivalências ingênuas entre prova analógica e prova digital-eletrônica, começando-se pela extração completa associada ao fornecimento à parte adversa (acusação ou defesa). Do contrário, abre-se espaço para práticas oportunistas que, todavia, deixam rastros. Mais cedo ou mais tarde, entretanto, a armadilha digital cai, afinal, quem tem medo de entregar a extração completa? Só quem tem algo a esconder. E isso é incompatível com o devido processo legal digital.

P.S. Parabéns ao colega Antônio Gavazzoni, aniversariante da semana, que além de defender seu segundo doutorado em Direito, procurou-nos para aprender sobre prova digital desde o início, a partir da constatação de que o mundo da prova digital revolucionou o processo judicial e, por isso, é hora de se reinventar. Seja bem-vindo. Quanto antes, melhor. Conte conosco.

Fonte: https://conjur.jumps.com.br/2025-ago-22/prova-digital-comprometida-pela-simples-alteracao-da-data-no-dispositivo-apreendido/