# O “print screen” e a materialidade nos crimes digitais

– 1. **Escopo**. O texto sustenta que o "print screen" é insuficiente à demonstração da materialidade dos ital/eletrônico (definição e tratamento).

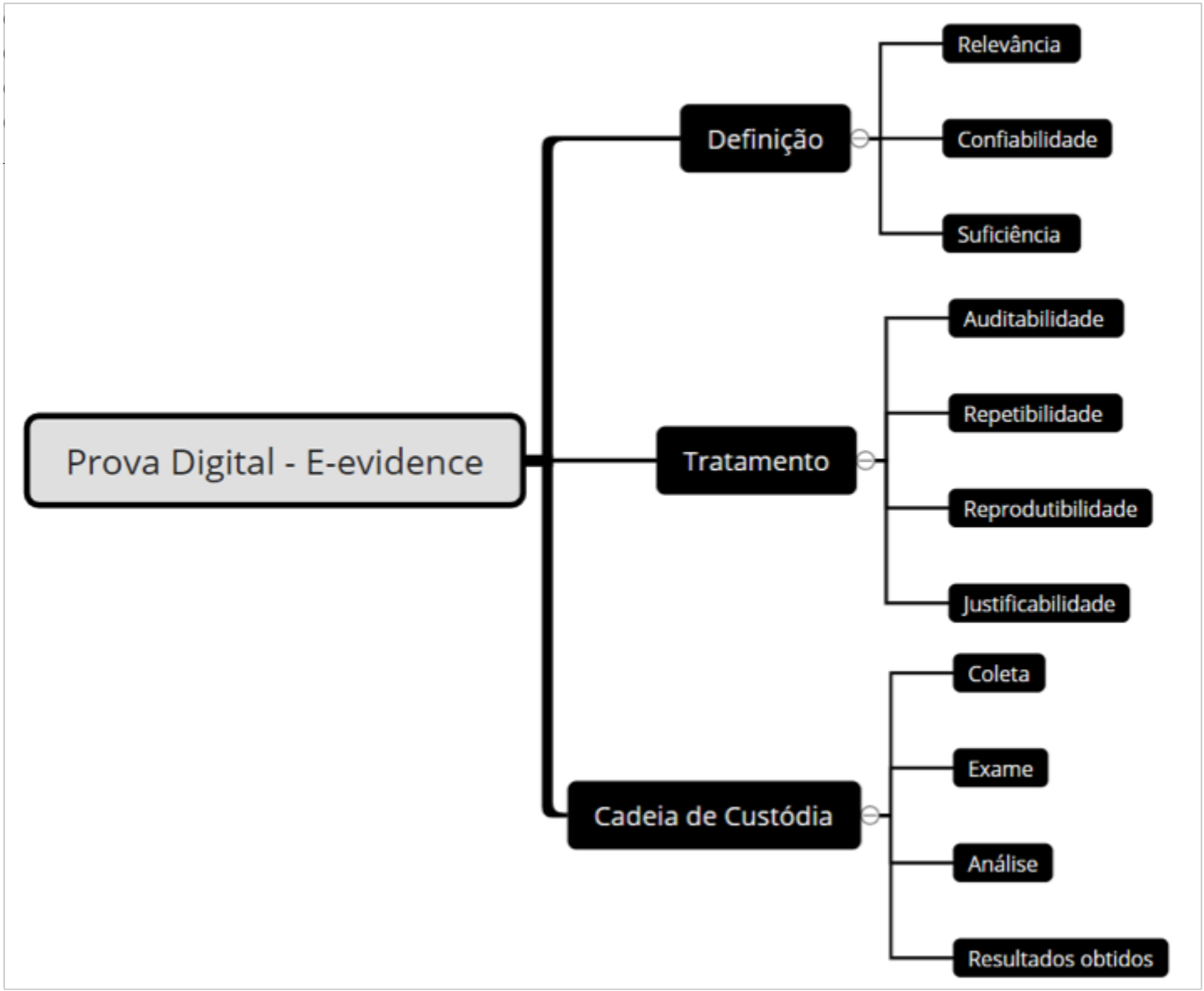

– 2. **Prova Digital (*e-evidence*)**. A prova digital (espécie da prova eletrônica) é a obtida e/ou produzida em ambiente eletrônico digital, em que os dados (*de base, de tráfego e de conteúdo*), em geral, vulneráveis, intangíveis e frágeis, devem ser extraídos e tratados em observância às normas técnicas, observada a cadeia de custódia digital, sob pena de ineficácia probatória. A tendência contemporânea é a do uso futuro da tecnologia *blockchain*.

– 3. **Definição de *"e-evidence"***. A definição de *"e-evidence"* orienta-se pela: **(a)** relevância (*meio de prova adequado ao fim que se destina*); **(b)** confiabilidade (*equivalência entre o verificado e o representado*); e, **(c)** suficiência (*deve congregar os elementos necessários de superação aos testes de verificação*).

– 4. **Tratamento da *"e-evidence"***. Já o Tratamento da "e-evidência" deve ser realizado por cópia ( *aquisição*) e autorizar as seguintes condições: **(a)** auditabilidade (*conformidade da metodologia e dos procedimentos*); **(b)** repetibilidade (*os resultados obtidos, nas mesmas condições, devem ser os mesmos*); **(c)** reprodutibilidade (*equivalência de resultados por meio de instrumentos diversos*); e, **(d)** justificabilidade (*justificação da escolha e realização dos procedimentos e métodos de obtenção e tratamento*).

– 5. **Cadeia de Custódia**. Considerando as características dos dados alvo da prova (volatilidade e fragilidade), a evidência digital pode ser alterada, editada, manipulada ou destruída de modo doloso ou culposo, tanto pelos agentes processuais, como pelos peritos. A "e-evidência" constitui-se pelos formatos físico e lógico. Desde o rastreio e a obtenção, até o descarte, todo o percurso e tratamento deve ocorrer

com a "identificação" dos dispositivos (externa, via dispositivo de armazenamento e, se possível e viável, a interna: os dados), evitando-se sobreposições. Os cuidados com a Cadeia de Custódia Digital (controle de obtenção, movimento e acesso aos dados, com a identificação, histórico de acesso, por tempo, local e motivação, além de eventuais alterações) se potencializam, porque é dever de todos os agentes que participam da obtenção ou tratamento da evidência digital, além de conhecimentos mínimos (p.ex. o programa MD5Summer verifica a integridade dos arquivos transmitidos pela web), a respectiva documentação das condições matérias do rastreamento, identificação, fixação, aquisição (cópia integral e



– 6. **Materialidade nos crimes que deixam vestígios**. A materialidade é indispensável nos crimes que deixam vestígios (CPP, artigo 158), os praticados por meio digital/eletrônico exigem a observância das normas técnicas de existência, de validade e de eficácia. A prova digital (*e-evidence*) depende da aquisição válida dos dados e não somente da imagem (da aparência visível). Eis um dos desafios atuais do regime probatório digital.

– 7. **Aquisição de Dados**. A aquisição e/ou extração de dados do ambiente digital, especificamente da internet ou de aplicativos de mensageria, deve observar os requisitos de Existência, Validade e Eficácia (Teste EVE). A aplicação analógica do artigo 411, II, do CPC (*Art. 411. Considera-se autêntico o documento quando: […] II – a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei.*) autoriza a invocação das regras técnicas (ABNT-ISO) como parâmetro de verificação da autenticidade.

– 8. **Regras Técnicas**. As Regras Técnicas (Norma ABNT ISO/IEC 27.037:201) são de observância obrigatória. A Organização Internacional de Padronização (ISO) editou a Norma ABNT NBR ISO/ IEC 27037:2013, estabelecendo os critérios de tratamento das evidências digitais, isto é, os requisitos de existência e de validade à preservação da integridade, da autenticidade, da auditabilidade e da cadeia de custódia relativas à evidência digital.

– 9. ***"Print Screen"***. Em consequência, o mero *"print screen"* é insuficiente à demonstração da materialidade, por violação da metodologia necessária à existência e à validade do suporte material, por violação dos elementos de "definição" e de "tratamento". É que os documentos nativos do ambiente digital demandam aquisição adequada dos dados, em geral por "imagem" (*no conceito técnico e não do "print screen", por evidente*). Logo, não preenche os atributos de Definição e de Tratamento.

– 10. **CPC e CPP**. Se no Processo Civil, em que os direitos, em geral, são "disponíveis" os *"prints"* impugnados são considerados "irrelevantes" e "inválidos", com maior rigor no Processo Penal, em que os direitos são indisponíveis.

– 11. **Manipulação**. O *"print screen"* pode ser manipulado amplamente. Os dados podem ser"montados" por meio de aplicativos disponíveis nas lojas dos smartphone (*google play* e *apple store*),"espoliados" ( *degradação por incidência de calor, umidade, campos magnéticos e/ou elétricos, quedas etc*.) ou "adulterados" (*violada a integridade, mesmidade e auditabilidade*), por aspectos inerentes àdiligência de aquisição ou pela interferência de agentes externos. Por isso que agentes profissionais,assim que o dispositivo é apreendido, promovem o desligamento ou a colocação em modo avião (*evitam a adulteração por administradores ou agentes externos*). As operações policiais seguem oprocedimento de imediata colocação e "modo avião". Por ser amplamente "manipulável", o *"print screen"* (*conjunto de pixels*), ao contrário do Processo Civil, em que a não contestação do réu, consolidaa autenticidade, no domínio do Processo Penal a "materialidade" exige a aquisição adequada, até porquea confissão é insuficiente.

– 12. **Ônus da Prova**. Se o ônus probatório é da acusação, o Estado ou o querelante devem adquirir validamente os dados, motivo pelo qual a não-conformidade significa a ausência de materialidade, pouco importando se a defesa deixa de impugnar o "print screen" ou mesmo confessa o envio da mensagem porque a confissão é inválida para o fim de comprovação da materialidade. A exigência é do regime probatório do Processo Penal (CPP, artigo 158; artigo 564, III, "b"). Em consequência, eventual confissão não supre a ausência de aquisição válida da prova.

– 13. **Ata Notarial**. A produção de Ata Notarial, para fins de validade, depende do preenchimento dos requisitos legais quanto à metodologia aplicável à extração dos dados. O instrumento público, por si, é in suficiente, porque será necessária a determinação dos indicadores capazes de atribuir integridade, autenticidade, auditabilidade, além de observar a cadeia de custódia. O conteúdo deve ser extraído da *web* e não de eventual *print* apresentado pelo requerente ou a narrativa do que é visualizado pelo notário. Em consequência, se os dados não forem adquiridos, a transcrição e/ou a narrativa, para fins penais, também serão insuficientes à configuração da materialidade.

– 14. **Extração válida**. A validade está vinculada à garantia de integridade do modo como se capturam os dados de tráfego, de vestígios e dados digitais (inclusive conversas de Whatsapp, Telegram, Facebook, Instagram, sítios online etc.), em atenção à cadeia de custódia. Estão disponíveis no mercado diversos produtos capazes de, com rapidez, eficiência e validade jurídica, promover a extração e documentação de conteúdo da web (Verificat, PACWeb, por exemplo, são bem funcionais).

– 15. **Um Julgado**. No julgamento da Apelação Criminal 5004504-77.2020.8.24.0079, em que fui relator, junto à 3ª Turma Recursal do TJ-SC, decidimos:

*"CRIME DE AMEAÇA (ART. 147, CAPUT, DO CÓDIGO PENAL). CONDENAÇÃO NA ORIGEM. PLEITO DEFENSIVO PELA ABSOLVIÇÃO POR INSUFICIÊNCIA DE PROVAS. PROMESSA DE CAUSAR MAL INJUSTO E GRAVE SUPOSTAMENTE PERPETRADA POR MEIO DE APLICATIVO DE MENSAGERIA (WHATSAPP). PROVA MATERIAL LIMITADA À JUNTADA DE CAPTURA DE TELA FORNECIDA PELA VÍTIMA. INSUFICIÊNCIA. VIOLAÇÃO DA METODOLOGIA DE AQUISIÇÃO VÁLIDA DA MATERIALIDADE NOS CRIMES QUE DEIXAM VESTÍGIOS (CPP, ART. 158). REGRAS DE DEFINIÇÃO E TRATAMENTO INOBSERVADAS. O "PRINT SCREEN" É INSUFICIENTE À MATERIALIDADE NECESSÁRIA À EXISTÊNCIA E À VALIDADE DA PROVA DIGITAL NO ÂMBITO CRIMINAL. REGISTRO QUE NÃO PERMITE NEM SEQUER A IDENTIFICAÇÃO DO INTERLOCUTOR. AUSÊNCIA DE MATERIALIDADE. ABSOLVIÇÃO NOS*

*TERMOS DO ART. 386, INCISO II, DO CÓDIGO DE PROCESSO PENAL QUE SE IMPÕE. RECURSO PROVIDO".*

– 16. **Em conclusão**. A apuração de condutas criminais que se valem do ambiente digital (próprias ou impróprias) exige comprovação adequada por meio da observância de regras, metodologias e procedimentos técnicos. Os *prints* extraídos de endereços da *web* ou de *smartphones* (Whatsapp, por exemplo), são qualificados como "imagem", submetido à demonstração do modo de obtenção e/ou produção. A maleabilidade e a vulnerabilidade dos dados digitais, principalmente pela ampla possibilidade de criação de diálogos falsos (*fakes*), por meio de aplicativos disponíveis na rede, reafirma a necessidade de observância da Cadeia de Custódia Digital. Diferentemente do regime do Processo Civil, em que a não impugnação pela parte adversa consolida a validade, no Processo Penal o ônus da prova é da acusação, motivo pelo qual a demonstração da existência, validade e eficácia é atribuída a quem acusa. O *print*, por si, sem a demonstração da regularidade (metadados, integridade, código Hash, quem, como, onde, atendidas as regras de identificação e coleta), não produz nenhum efeito probatório. Em geral, será preciso a análise do dispositivo, se possível de todos os interlocutores, dada a possibilidade de manipulação. Por consequência, se os dados não foram adquiridos, o *"print screen"* é insuficiente à demonstração da "existência" da materialidade, motivo pelo qual a ação penal não pode ser admitida e, caso tenha sido, o acusado deve ser absolvido, nos termos do artigo 386, II, do CPP.

**Date Created**
17/06/2022