Digitalização do processo penal e a cadeia de custódia como controle epistêmico

10/12/2023

O Processo Penal brasileiro, há muito, tem a prova dependente da memória como principal fonte probatória para fundamentar condenações. A forma do procedimento, inclusive, privilegia a produção e uso de depoimentos de testemunhas e envolvidos nos fatos objeto de investigação e denúncia. Daí que se afirma que o paradigma probatório atual do processo penal no Brasil é fundado em provas dependentes da memória, como o testemunho e o reconhecimento de pessoas.

Exatamente por esta razão é que boa parte da doutrina tem se debruçado sobre o estudo da memória humana, tendo chegado a importantes (ainda que parciais) conclusões acerca da falibilidade da memória e, por consequência, da necessidade de observância de controles epistêmicos adequados à utilização destas provas no Processo Penal.

Não é para menos. O erro judiciário é um dos maiores expoentes de como a utilização negligente e excessiva de provas dependentes da memória no processo penal pode causar sérios prejuízos às pessoas que se veem acusadas injustamente. Em decorrência deste fenômeno é que vemos surgir iniciativas como o Innocence Project e o Prova sob Suspeita, do IDDD.

Ter um processo penal tão subordinado a provas dependentes da memória, as quais são sabidamente sujeitas a diversas falhas (fenômeno de falsas memórias, irrepetibilidade de reconhecimento pessoal, fator "foco na arma" entre outros tantos) não é o ideal. Indo além, com a modernização cibernética da sociedade, podemos argumentar que a digitalização do processo penal se oferece como uma alternativa, ou até uma panaceia para este cenário, o remédio perfeito para a causa da doença, e não do sintoma. Entretanto, trata-se de uma conclusão ingênua, como se verá a seguir, já que a digitalização do processo vem acompanhada de problemas que lhe são próprios.

Eric Hilgendorf em seu texto *Digitalização e Direito (Penal): Apelo por uma Expansão de Perspectivas* [1] nos traz importantes conceitos (e alertas).

Em primeiro lugar, o autor conceitua a digitalização da informação como a *"representação de informações como zeros e uns"* [2]. O fenômeno da digitalização, então, pode ser entendido como o transporte do que temos no mundo analógico para este universo algorítmico, substituindo-se os papéis por arquivos, cartas por mensagens de WhatsApp, contratos celebrados presencialmente por assinados via e-mail e volumes de processos judiciais

impressos por PDFs nos processos eletrônicos de Tribunais.

A digitalização das interações entre indivíduos trouxe como consequência a digitalização de diversos crimes, bem como o surgimento de outras modalidades de delitos. Como o autor ressalta, a preocupação dos estudiosos costuma ser orientada à análise de novas infrações penais e novos métodos de investigação penal, contudo, essa é uma visão rasa do fenômeno da digitalização do Direito Penal. Ao que nos interessa, especialmente, esta visão restrita desconsidera todos os efeitos que a digitalização teve, tem e seguirá tendo para o funcionamento do Processo Penal. Como diplomas legais relevantíssimos, mencionamos o Marco Civil da Internet, e, mais recentemente, a LGPD. Essas leis corporificam a compreensão do nosso Poder Público acerca da necessidade de tutela sobre o mundo digitalizado.

Muito embora a utilização de provas digitais não seja um fenômeno recente (a computação forense é uma área de estudo que já existe há décadas), para o Brasil, foi com o advento da operação "lava-jato" que o tema ganhou destaque na doutrina e na jurisprudência. Em especial, gostaríamos de eleger como marco o momento em que a força-tarefa torna evidente sua cooperação internacional com a empresa responsável pela fabricação de aparelhos Blackberry, já em 2015 [3], e um dos temas discutidos mais fervorosamente à época dizia respeito à (1) legalidade do acesso às mensagens pelo aplicativo BBM [4][5].

Para além do funcionamento analógico do Processo Penal, aqui, evidenciou-se um novo modelo de persecução penal, onde o protagonismo se dirige às provas digitais, e as provas dependentes da memória, por sua vez, tornam-se coadjuvantes, servindo enquanto instrumentos para construção do mosaico probatório, amarrando quem fez o quê, para quem, onde e quando. Hoje, os termos "arquivos em nuvem/*cloud*", "código *hash*", "mídias acauteladas", entre tantos outros, já se tornaram lugar-comum para a advocacia criminal.

Como bem sabemos, a "lava jato" foi permeada por dezenas de atropelos antigarantísticos, e é um cristalino exemplo de como *não* conduzir uma persecução penal. Após inúmeras anulações, vê-se que a "lava jato" cometeu diversos erros que culminaram em muitas condenações indevidas. O mais emblemático caso, inclusive, é o da anulação das condenações proferidas pela 13ª Vara Federal de Curitiba contra o atual presidente da República, Luiz Inácio Lula da Silva.

A bem da verdade, o problema da administração da Justiça Criminal, ao menos no que diz respeito à matéria probatória, não se encontra (apenas) nas falibilidades das provas dependentes da memória e na relação umbilical que o Processo Penal brasileiro tem com elas. Está, sim, na (ir)racionalidade punitivista e inquisitória que guia a investigação, a acusação e, na maior parte das vezes, toda a instrução criminal, contemplando-se aí a colheita, produção e valoração das provas sem que haja a menor preocupação com o controle da atividade probatória. Daí é que surge, então, a necessidade de sistemas de controle epistêmicos sobre a atividade probatória, e a indagação: como controlar a atividade probatória em um contexto de provas digitais?

A cadeia de custódia da prova

Como bem apontado por Morais da Rosa e Aury Lopes Jr., o eixo central do processo penal é a prova — por meio da prova que se fará a recognição de um fato passado, para que o juiz possa

proferir no presente uma decisão que projetará efeitos futuros [6].

A cadeia de custódia passou a ser legalmente tutelado no Brasil com o advento do pacote anticrime, e se encontra prevista nos artigos 158-A a 158-F, do Código de Processo Penal. Começamos a exposição sobre o tema com a análise do HC 160.662/RJ, que tramitou perante o Superior Tribunal de Justiça. O *writ* tratava principalmente da nulidade das interceptações telefônicas e telemáticas pela alegada quebra na cadeia de custódia.

Naquele caso, muito embora a defesa tenha tido acesso aos autos do processo, parte das provas obtidas a partir da interceptação telefônica se perdeu, e assim, como consta na decisão, "*o conteúdo dos áudios telefônicos não foi disponibilizado da forma como captado, havendo descontinuidade nas conversas e na sua ordem, com omissão de alguns áudios*". Neste julgado importantíssimo, no qual foi acolhida tese paradigmática do professor Geraldo Prado sobre a quebra da cadeia de custódia da prova, ficou sedimentado que a não disponibilização da integralidade da prova à defesa fere a paridade de armas, inviabilizando o pleno exercício do contraditório e da ampla defesa, ante a impossibilidade de refutação da tese acusatória que essa indisponibilidade causa.

Como dito em palestra recente pela professora Janaína Matida, "*não existe cadeia de custódia de prova dependente da memória*" [7]. Por outro lado, quando tratamos de provas produzidas fora do ambiente processual, a cadeia de custódia não apenas existe como é condição necessária para conferir fiabilidade àquela prova [8].

A prova digital, vale ressaltar, é volátil, especialmente sujeita a modificações e perdas em comparação aos meios de prova tradicionais. Por esta razão, inclusive, é que há ampla produção intelectual no sentido de sedimentar boas práticas no campo da computação forense para o trato de provas em meio digital.

Diante desta complexidade, bem como considerando o próprio rito de colheita e cautela das provas digitais, é que a devida observância da cadeia de custódia se evidencia como imprescindível quando tratamos de provas digitais [9]. Isto porque somente a adequada documentação da cadeia de custódia desta prova conseguirá assegurar sua autenticidade e integralidade, possibilitando o escrutínio da mesma em sede judicial, de modo a preservar a ampla defesa e o contraditório [10]. Segundo Gustavo Badaró, "*A necessidade de documentação da cadeia de custódia é fundamental para assegurar o potencial epistêmico das fontes de prova reais*".

Mais recentemente, o STJ ao analisar o AgRg no Recurso Ordinário em Habeas Corpus nº 143.169 proveu o Agravo Regimental, para declarar a inadmissibilidade das provas digitais no caso concreto.

No ponto, merece especial destaque o voto proferido pelo ministro Ribeiro Dantas, que divergiu do então relator (desembargador convocado do TJ-DF, Jesuíno Rissato), observando que as provas imateriais naquele feito exigem da polícia um elevado grau de conhecimento. No caso concreto, aduziu o ministro que após a apreensão dos computadores da quadrilha, seria necessário fazer uma cópia ou espelhamento, "*obtendo bytescreen mantendo a integridade*".

Entendeu o ministro Ribeiro Dantas naquele caso que houve descuido em relação aos aparelhos coletados no processo. Após uma explicação detalhada sobre o procedimento de cópia de imagem de computador, pontuou que "*Todo processo técnico deve ser documentado e registrado. A documentação da cadeia de custódia é essencial no caso da análise de dados digitais, porque permitirá assegurar a autenticidade e integralidade dos elementos de prova (...) e excluirá o que tenha tido alterações indevidas do material digital*".

No julgamento, concluiu-se que houve séria ofensa ao artigo 158 do Código de Processo Penal, com a quebra da cadeia de custódia dos computadores apreendidos, e que não havia nada que garantisse a idoneidade das provas produzidas pela polícia.

O *hash* e sua relevância para a cadeia de custódia da prova digital
Aplicando-se uma técnica de algoritmo *hash*, é possível obter uma assinatura única para cada arquivo — uma espécie de impressão digital ou DNA, por assim dizer, do arquivo. Esse código *hash* passaria a ter um valor diferente caso um único *bit* de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia, o que só é possível conferir mediante prova pericial. Para este fenômeno, pelo qual mínimas alterações acarretam em alteração do código *hash,* dá-se o nome de *efeito avalanche*.

Johan Matos Coelho da Silva e Philipe Matos Coelho da Silva definem que as funções *hash* são algoritmos matemáticos determinísticos que mapeiam dados de comprimento aleatório em saída de tamanho fixo em base hexadecimal, dispersando os *bits* de entrada de forma não correlacionada às mudanças. Ou seja, uma pequena mudança na entrada, seja um simples caractere em uma frase inteira, ou um pixel em uma foto, acarreta uma saída completamente diferente, sendo essa característica conhecida como *efeito avalanche* [11].

Desse modo, comparando as *hashes* calculadas nos momentos da coleta e de eventual perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi alterado, mesmo minimamente. Não havendo alteração (isto é, permanecendo íntegro o corpo de delito), as *hashes* serão idênticas, o que permite atestar com elevadíssimo grau de confiabilidade que a fonte de prova permaneceu intacta.

Disso resulta uma conclusão contraintuitiva: uma fonte de prova que armazena dados imateriais, *se* coletada de maneira profissional e técnica pela Polícia, pode oferecer garantias de mesmidade superiores àquelas de uma fonte corpórea (como um cadáver ou armamento de fogo), dada a precisão e objetividade do algoritmo de *hash*. Isso, claro, exige da polícia um elevado grau de conhecimento e diligência em sua atividade, devendo manter-se atualizada com as melhores práticas e documentar sua realização.

Para corroborar nossas conclusões quanto à obrigatoriedade dos procedimentos acima explicados, recorremos ao professor Gustavo Badaró [12], segundo o qual é imprescindível que o método empregado garanta a integridade do dado digital e, com isso, a força *probandi* do conteúdo probatório por ele representado. Normalmente, é necessário fazer uma cópia ou "espelhamento", obtendo o *bitstream* da imagem do disco rígido ou suporte de memória em que o dado digital está registrado. Além disso, por meio de um cálculo de algoritmo de *hash*, é possível verificar a perfeita identidade da cópia com o arquivo original. Com isso, de um lado,

se preserva o material original e, de outro, se garante a autenticidade e integridade do material que foi examinado pelos peritos. Evidente que esse processo técnico precisa ser documentado em todas as suas etapas. Tal exigência é uma garantia do correto emprego das *operating procedures*, especialmente por envolver um dado probatório volátil e sujeito à mutação. Exatamente pela diferença ontológica da prova digital com relação à prova tradicional, bem como devido àquela não se valer de uma linguagem natural, mas digital, é que uma cadeia de custódia detalhada se faz ainda mais necessária. Realmente, a documentação da cadeia de custódia é essencial no caso de análise de dados digitais, porque permitirá assegurar a autenticidade e integralidade dos elementos de prova e submeter tal atividade investigativa à posterior crítica judiciária das partes, e excluirá que tenha havido alterações indevidas do material digital.

Em um cenário de digitalização do processo penal, a preservação da cadeia de custódia como sistema de controle epistêmico da prova digital se revela, portanto, mais importante do que nunca.

---

[1] HILGENDORF, Eric. Digitalização e Direito. São Paulo: Marcial Pons, 2015. p. 25 e ss.

[2] *Ibid.*

[3] CANÁRIO, Pedro. Relação direta entre PF e empresa canadense alarma advogados da "lava jato". https://shorturl.at/AFLMS Revista CONJUR. Publicado em 10/11/15.

[4] REDAÇÃO CONJUR. Criminalistas criticam uso de provas na "lava jato" enviadas ilegalmente. https://shorturl.at/ilnL5 Publicado em 04/02/16.

[5] A questão de criptografia e segurança das mensagens enviadas pelo aplicativo BBM, da Blackberry, causou tanta comoção que se tornou uma verdadeira crise de Relações Públicas para a empresa. Mais em: https://shorturl.at/fwMT6

[6] ROSA, Alexandre Morais da. LOPES JR., Aury. A importância da cadeia de custódia da Prova Penal. Revista Consultor Jurídico. https://shorturl.at/aduP5 Acesso em 28/11/23.

[7] Palestra "Desvendando as provas digitais no processo penal". O evento pode ser assistido em sua integralidade a partir do seguinte link:
https://www.youtube.com/watch?v=fFEstq8b2Vw

[8] ROSA, Alexandre Morais da. LOPES JR., Aury. op. cit.

[9] BADARÓ, Gustavo. A cadeia de custódia da prova digital. https://shorturl.at/syFHR Acesso em 28/11/23.

[10] *Ibid.*

[11]SILVA, Johan Matos Coelho da; SILVA, Philipe Matos Coelho da. Técnicas de detecção e classificação de malwares baseada na visualização de binários. Monografia. UnB, 2018, p. 20-21.

[12] Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. Boletim IBCCRIM, 2021, p. 2.