Aplicação da cadeia de custódia da prova digital

A cadeia de custódia da prova penal[1] já foi objeto desta coluna, no final do ano passado (veja aqui), pouco antes da sanção presidencial quanto ao chamado “pacote anticrime”.

Sabe-se, portanto, que sem o devido “registro histórico” [2] do vestígio criminal, assim entendido “todo objeto ou material bruto, visi?vel ou latente, constatado ou recolhido, que se relaciona a? infrac?a?o penal” (artigo 158-A, § 3º, do CPP), desaparece qualquer garantia de sua regularidade epistêmica como fonte de conhecimento válido no processo penal.

Oportuno mencionar, na linha sustentada pelo professor Geraldo Prado, dois relevantes princípios de controle epistêmico sobre a autenticidade probatória enquanto premissa de fiabilidade, quais sejam, (i) a “mesmidade” e (ii) a “desconfiança”. Valendo-se de lições da doutrina processual penal colombiana e chilena, o mestre brasileiro considera esses postulados basilares “para garantir o juízo mediante a redução dos riscos de erro judiciário, consistindo no fundamento lógico e epistemológico da ‘cadeia de custódia das provas’”.[3]

Conforme Urazán Bautista, a cadeia de custodia é um sistema baseado em um princípio universal de autenticidade da prova, a chamada "lei da mesmidade" ("*ley de la mismidad*"), pela qual se determina que o "mesmo" ("*lo mismo*") que se encontrou no local de crime é "o mesmo" ("*lo mismo*") que se está utilizando para a tomada de uma decisão judicial.[4] Quanto ao segundo princípio, também fundamento da cadeia de custódia, afirmam Baytelman e Duce que não existem confianças preestabelecidas no campo da prova penal. Logo, um mero objeto ou documento apresentado em juízo não possui, em si mesmo, informação de qualidade suficiente para que se possa afirmar de forma segura que seja efetivamente aquilo que a parte encarregada daquela prova diz sê-lo. Ninguém, inclusive o juiz, tem que depositar confiança especial em quaisquer dos sujeitos processuais. Tudo deve ser aferido a partir das regras do campo probatório penal; fora do mundo da prova não podem existir concessões para nada, o que alcança as proposições fáticas a respeito do que seja (ou não) algum documento ou objeto exibido em juízo.[5]

Nesse contexto, importante ressaltar que, embora normalmente relacionada à prova científica e, mais especificamente, à perícia de laboratório, a aplicação da cadeia de custódia deve ser entendida de forma mais ampla, abarcando qualquer fonte de prova de natureza real, conforme a lição de Badaró . Não se limita, portanto, às coisas "materiais" (ex.: uma faca ou um fragmento de munição). Também necessária a observância da cadeia de custódia em face de "elementos 'imateriais' registrados eletronicamente, como o conteúdo de conversas telefônicas, ou de transmissão de e-mail, mensagens de voz, fotografias digitais, filmes armazenados na internet etc".[6]

Aliás, essa preocupação com a garantia de originalidade dos vestígios imateriais tende a ser cada vez mais recorrente no sistema de justiça penal.[7] O motivo é por todos conhecido: a frequente interseção direito e tecnologia, especialmente no campo investigativo criminal, com a profusão de métodos ocultos de pesquisa.[8]

A esse respeito, vale citar como exemplo a legislação italiana. São algumas as referências expressas no *Codice di Procedura Penale*, ainda que de forma pontual, sobre a questão da fiabilidade probatória no campo digital (ex.: artigos 244.2, 247.1-bis, 254-bis.1, 352.1-bis e 354.2). Um tema, sem dúvida alguma, bastante importante dado o elevado risco de adulteração das fontes de prova imaterial, em especial da chamada *digital evidence****[9]***.

Deveras, as características ímpares da prova digital tornam-na tecnicamente complexa e carente de leitura especializada, sobretudo em respeito à necessária "integridade, fiabilidade e inalterabilidade" dos elementos probatórios, o que se busca assegurar pela manutenção dos procedimentos atinentes à "cadeia de controlo" na linguagem portuguesa.[10]

Muito embora não se tenha no Código de Processo Penal brasileiro nenhuma disciplina específica quanto aos procedimentos a serem observados no tocante à cadeia de custódia de vestígio digital, existem diretrizes estabelecidas pela Associação Brasileira de Normas Técnicas (ABNT) que podem orientar o sistema de justiça criminal nesse moderno campo da integridade probatória. As regras em questão podem ser extraídas da norma ABNT NBR ISO/IEC 27037:2013, que entrou em vigor na data de 09 de janeiro de 2014, versando especificamente sobre os procedimentos de identificação, coleta, aquisição e preservação de evidência digital.[11]

Outras importantes referências metodológicas nessa área podem ser extraídas de conhecido documento técnico (RFC) criado pelo grupo internacional *Internet Engineering Task Force* (IETF). Trata-se da RFC

3227 – Diretrizes para a Coleta e Arquivamento de Evidências –, cujo tópico 4.1. alude especificamente à cadeia de custódia, de modo que se tenha a documentação precisa a respeito de onde, quando e por quem a(s) evidência(s) foi(ram) descoberta(s) e coletada(s), tratadas ou examinadas, durante qual lapso temporal, de qual modo, bem como quando e como houve mudança na relação de custódia.[12]

O que se justifica exatamente pela necessidade de se garantir as características fundamentais de uma evidência computacional. Aliás, segundo a referida Força Tarefa de Engenharia da Internet (IETF), essas evidências precisam ser: i) admissíveis (em consonância com as regras legais que validem sua admissão em juízo); ii) autênticas ou íntegras (serem as mesmas evidências coletadas originalmente no local do evento); iii) completas (permitirem a narrativa de todo o evento, e não somente uma visão particular do observador); iv) confiáveis (terem a capacidade de gerar crenças verdadeiras); e v) críveis (compreensíveis pelos seus destinatários).[13]

Já no âmbito específico da perícia criminal brasileira, vale mencionar o procedimento operacional padrão do Ministério da Justiça, cujo item 3.1. se destina à informática forense, mais especificamente ao exame pericial de mídia de armazenamento computacional.[14] O que, no fundo, é algo próprio da nossa época, marcada pela "técnica da informação", por meio da cibernética, da internet e da eletrônica, com duas características igualmente relevantes, quais sejam, a aceleração do processo histórico e seu considerável potencial invasor.[15]

Não custa frisar, ainda, retornando à leitura estrita do campo processual penal, que também quanto aos vestígios imateriais a preservação do local de crime é fundamental e, via de regra, incumbe prioritariamente aos órgãos policiais. Aliás, essa fase inicial da cadeia de custódia do vestígio digital é de suma importância para garantir a idoneidade dos elementos probatórios. Não por outro motivo a grande preocupação, por exemplo, do departamento de justiça estadunidense quanto à conduta dos agentes públicos que têm o primeiro contato com esses espaços delitivos.[16]

De fato, esse "caráter manipulável das provas eletrônicas"[17] deveria ser objeto de maior preocupação do sistema processual penal. É preciso ter bastante claro que "dados e metadados podem ser facilmente alterados, adulterados, suprimidos, inseridos e/ou corrompidos".[18] Os riscos de falsificação, erro, uso indevido ou abuso "são especialmente frequentes e relevantes"[19] quanto às evidências informáticas. Por conseguinte, a exigência de padrões rigorosos quanto à cadeia de custódia dos vestígios imateriais, especialmente no campo digital,[20] figura como mecanismo essencial de controle da necessária "integridade, fiabilidade, inalterabilidade e auditabilidade"[21] desses elementos probatórios cada vez mais frequentes na justiça criminal.

[1] A cadeia de custódia foi definida em lei como "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento ate? o descarte" (artigo 158-A, *caput*, do CPP).

[2] BORRI, Luiz Antônio; ÁVILA, Gustavo Noronha de. A cadeia de custódia da prova no "projeto de

lei anticrime": suas repercussões em um contexto de encarceramento em massa. *Revista Direito Público* , v. 16, n. 89, p. 114-132, set./out. 2019, p. 119.

[3] PRADO, Geraldo. *A Cadeia de Custódia da Prova no Processo Penal.* São Paulo: Marcial Pons, 2019, p. 97.

[4] BAUTISTA, Juán Carlos Urazán. *La Cadena de Custodia en el Nuevo Código de Procedimiento Penal*. Disponível em: <https://fundacionluxmundi.com/custodia.php>. Acesso em: 19.01.2020.

[5] BAYTELMAN, Andrés; DUCE, Mauricio J.. *Litigación Penal, Juicio Oral y Prueba*. México: Fondo de Cultura Económica, 2005, p. 284 *apud* PRADO, Geraldo. *A Cadeia de Custódia da Prova no Processo Penal...*, p. 95.

[6] BADARÓ, Gustavo. A Cadeia de Custódia e sua Relevância para a Prova Penal. In: SIDI, Ricardo; LOPES, Anderson Bezerra (Org). *Temas Atuais da Investigação Preliminar no Processo Penal*. Belo Horizonte: Editora D'Plácido, 2017, p. 522.

[7] Na mesma linha: MACHADO, Vitor Paczek; JEZLER JUNIOR, Ivan. A prova eletrônico-digital e a cadeia de custódia das provas: uma (re)leitura da Súmula Vinculante 14. *Boletim IBCCRIM*, São Paulo, ano 24, n. 288, nov./2016, p. 8-9 / SANTORO, Antonio Eduardo Ramires; TAVARES, Natália Lucero Frias; GOMES, Jefferson de Carvalho. O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 3, n. 2, p. 605-632, mai./ago. 2017.

[8] ARMENTA DEU, Teresa. Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre. *IDP: Revista d'Internet, Dret i Política*, Catalunya, n. 27, p. 67-79, set. 2018.

[9] "(…) digital evidence is defined as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi (adapted from Chisum, 1999)" (CASEY, Eoghan. *Digital Evidence and Computer Crime: forensic science, computers and the internet*. 03 ed. New York: Elsevier, 2011, p. 07).

[10] AGUIAR, Tiago Leonel dos Santos. *O Correio Eletrónico: a apreensão e a interceção no processo penal português*. 2017. Dissertação (Mestrado) – Universidade de Coimbra, Faculdade de Direito, p. 41-42.

[11] PARODI, Lorenzo. A cadeia de custódia da prova digital à luz da lei 13.964/19 (Lei anticrime). Disponível em: <https:// www.migalhas.com.br/depeso/320583/a-cadeia-decustodia-da-prova-digital-a-luz-da-lei-13964-19-leianticrime

>. Acesso em: 17.02.2020.

[12] IETFC. RFC 3227 – Guidelines for Evidence Collection and Archiving. 4.1 Chain of Custody. Disponível em: <https://www.ietf.org/rfc/rfc3227.txt>. Acesso em: 21.03.2020.

[13] IETFC. RFC 3227 – Guidelines for Evidence Collection and Archiving. 2.4 Legal Considerations. Disponível em: <https://www.ietf.org/rfc/rfc3227.txt>. Acesso em: 21.03.2020.

[14] BRASIL. *Procedimento Operacional Padrão. Perícia Criminal*. Brasília: Ministério da Justiça, 2013, p. 87-91.

[15] SANTOS, Milton. *Por Uma Outra Globalização: do pensamento único à consciência universal*. 06 ed. Rio de Janeiro, 2001, p. 24-27. Conclui o autor: "Há uma relação de causa e efeito entre o progresso técnico atual e as demais condições de implantação do atual período histórico. É a partir da unicidade das técnicas, da qual o computador é uma peça central, que surge a possibilidade de existir uma finança universal, principal responsável pela imposição a todo o globo de uma mais-valia mundial. Sem ela, seria também impossível a atual unicidade do tempo, o acontecer local sendo percebido como um elo do acontecer mundial. Por outro lado, sem a mais-valia globalizada e sem essa unicidade do tempo, a unicidade da técnica não teria eficácia" (SANTOS, Milton. *Por Uma Outra Globalização: do pensamento único à consciência universal*. 06 ed. Rio de Janeiro, 2001, p. 27).

[16] U.S. DEPARTMENT OF JUSTICE. *Electronic Crime Scene Investigation: a guide for first responders*. 02 ed. Washington/DC: National Institute of Justice, 2008.

[17] PRADO, Geraldo. *A Cadeia de Custódia da Prova no Processo Penal*. São Paulo: Marcial Pons, 2019, p. 110.

[18] VIEIRA, Thiago. Aspectos Técnicos e Jurídicos da Prova Digital no Processo Penal. Disponível em: <http://www.ibadpp.com.br/aspectos-tecnicos-e-juridicos-da-prova-digital-no-processo-penal-por-thiago-vieira/>. Acesso em 21.03.2020.

[19] TARUFFO, Michele. *A Prova*. Trad. João Gabriel Couto. São Paulo: Marcial Pons, 2014, p. 84.

[20] "Chain of custody and integrity documentation are important for demonstrating the authenticity of digital evidence. Proper chain of custody demonstrates that digital evidence was acquired from a specific system and/or location, and that it was continuously controlled since it was collected. Thus, proper chain of custody documentation enables the court to link the digital evidence to the crime. Incomplete documentation can result in confusion over where the digital evidence was obtained and can raise doubts about the trustworthiness of the digital evidence" (CASEY, Eoghan. *Digital Evidence and Computer Crime: forensic science, computers and the internet*

. 03 ed. New York: Elsevier, 2011, p. 60).

[21] VIEIRA, Thiago. Aspectos Técnicos e Jurídicos da Prova Digital no Processo Penal. Disponível em: <http://www.ibadpp.com.br/aspectos-tecnicos-e-juridicos-da-prova-digital-no-processo-penal-por-thiago-vieira/>. Acesso em 21.03.2020.

Date Created
31/03/2020