Lorenzo Parodi: A cadeia de custódia da prova digital

A cadeia de custódia pode ser definida como o conjunto de procedimentos documentados que registram


trole, transferência, análise e eventual descarte de evidências.

O conceito de preservação da cadeia de custódia no processo penal diz respeito à garantia de integridade e, por consequência, credibilidade e prestabilidade da prova, mas, também, ao exercício do contraditório pelas partes que devem ter acesso a una prova certamente íntegra, sem esquecer o juiz, que é o destinatário da prova.

A atenção à cadeia de custódia no processo penal é comum e crescente em muitos países. Da mesma forma, no Brasil, a preservação da cadeia de custódia e a necessidade de considerar imprestável a prova quando sua cadeia de custódia tiver sido quebrada, por se tratar, nesse caso, de prova de integridade duvidosa, pois contaminada até pela simples possibilidade de adulteração, foram objeto de importantes estudos jurídicos cujas teses foram acolhidas, em muitos casos, pelas cortes brasileiras e acabaram formando jurisprudência.

Destacam-se, neste sentido, os brilhantes e profundos estudos e obras do preclaro professor Geraldo Prado, certamente o pioneiro no Brasil das teses envolvendo cadeia de custódia.

Finalmente, com o advento da Lei 13.964/2019 (lei "anticrime") e a consequente introdução no CPP dos Artigos 158-A até 158-F, apareceu a primeira formal e legal definição de cadeia de custódia e o reconhecimento de sua relevância.

De acordo com a mencionada lei, a cadeia de custódia das evidências (ou vestígios) compreende, resumidamente, os seguintes procedimentos ou etapas:

I — *Reconhecimento*: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;

II — *Isolamento*: ato de evitar que se altere o estado das coisas;

III — *Fixação*: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito;

IV — *Coleta*: ato de recolher o vestígio, respeitando suas características e natureza;

V — *Acondicionamento*: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, com anotação da data, hora e nome de quem realizou a coleta;

VI — *Transporte*: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas, de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;

VII — *Recebimento*: ato formal de transferência da posse do vestígio, que deve ser documentado;

VIII — *Processamento*: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada;

IX — *Armazenamento*: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado;

X — *Descarte*: procedimento referente à liberação do vestígio, mediante autorização judicial.

Importante, também, destacar que, de acordo com o artigo 158-A, §2º, instituído pela supracitada lei "anticrime", *"o agente público que reconhecer um elemento como de potencial interesse para a produção da prova pericial fica responsável por sua preservação"*.

É importante observar que a Lei 13.964/2019, após uma definição introdutiva geral do conceito de cadeia de custódia, foca sobretudo nos procedimentos a serem aplicados para o caso de evidências físicas e materiais, tratando de questões como sua descrição e posição no local do crime, sua coleta e acondicionamento de acordo com as características físicas, químicas e biológicas etc.

Fica evidente que foram tomados cuidados na descrição detalhada dos procedimentos relativos à cadeia de custódia de evidências típicas de certos tipos penais, mas não foram tratados os procedimentos relativos a outros tipos de evidências, igualmente comuns, sobretudo em outros tipos penais.

Estou me referindo, em especial, às evidências digitais, tão comuns em casos de corrupção, lavagem de dinheiro e crimes econômicos em geral, mas que, com a evolução e difusão da tecnologia, hoje aparecem também em investigações relativas a tipos penais como roubo, tráfico, sequestro e outras "tradicionais" atividades criminosas organizadas.

Refletindo sobre tal aparente omissão, em uma lei promovida num momento de grandes casos de corrupção e lavagem de dinheiro, repletos de provas digitais, cheguei à conclusão de que, na realidade, pode se tratar de uma escolha intencional, inteligente, racional e perfeitamente explicável.

De fato, definir em lei procedimentos técnicos relativos à cadeia de custódia de evidências digitais poderia ser inútil ou até contraproducente, pois, num ambiente de rápida e constante evolução tecnológica, haveria grande chance de tais procedimentos ficarem rapidamente ultrapassados e não mais

conformes às melhores práticas.

Por essa razão, é certamente melhor criar uma lei, como aquela em foco, que defina conceitos e critérios de cunho geral, remetendo a normas técnicas de mais fácil atualização, a definição detalhada dos procedimentos relativos a âmbitos em constante evolução, como o mundo digital.

Quais deverão ser, então, os procedimentos a serem adotados em relação à cadeia de custódia de evidências digitais, no que diz respeito a conceitos, aspectos e etapas gerais definidas na referida lei, mas não diretamente aplicáveis a evidências digitais na forma em que foram descritos em tal lei?

Nos socorre, neste caso, a norma ABNT/ISO 27037, em vigor no Brasil desde janeiro de 2014 e que se coaduna perfeitamente ao caso.

Tal norma, redigida pela ABNT (Associação Brasileira de Normas Técnicas, órgão responsável pela normalização técnica no Brasil) com base na equivalente norma internacional elaborada pelo ISO (*International Organization for Standardization*), descreve e define as "Diretrizes para identificação, coleta, aquisição e preservação de evidência digital".

Apesar de não se tratar de norma cogente, por não haver, ainda, um reconhecimento explícito em lei, é, de fato, a única norma elaborada por organismo competente e reconhecido no Brasil, que trate explicitamente do assunto em foco, além de ser a norma que, em sua versão internacional (ISO), descreve os procedimentos adotados de direito ou "de facto" nos ordenamentos de muitos países.

Por essas razões, considerando de um lado, a existência da necessidade legal, em força do disposto pela mencionada Lei 13.964/2019, de realizar adequados e documentados procedimentos de identificação, coleta, aquisição e preservação de evidências (cadeia de custódia), e, por outro lado, a ausência de uma descrição detalhada de tais procedimentos para o caso de evidências digitais, entendo que seja perfeitamente possível defender a plena e necessária aplicabilidade da norma ABNT 27037 para a descrição dos procedimentos necessário para garantir a de cadeia de custódia de evidencias digitais.

Mas o que diz, afinal, a norma ABNT 27037?

O intuito aqui não é reproduzir um documento normativo com 50 páginas, mas resumir alguns dos aspectos de maior relevância.

A norma define quatro aspectos-chave no manuseio da evidência digital: auditabilidade, justificabilidade e repetibilidade ou reprodutibilidade (dependendo das circunstâncias particulares).

O processo de manuseio, por sua vez, é composto pelas seguintes etapas: identificação, coleta, aquisição e preservação.

Nesta sede concentrarei a atenção em dois desses procedimentos ou etapas, frequentemente fonte de problemas, a identificação e a preservação.

Com relação à identificação é oportuno, destarte, observar que a evidência digital é representada na forma física e lógica. A forma física inclui a representação de dados dentro de um dispositivo tangível. A forma lógica da evidência digital refere-se à representação virtual dos dados dentro do dispositivo.

O processo de identificação envolve a pesquisa, reconhecimento e documentação da evidência digital. É importante que o processo de identificação inicie identificando o armazenamento da mídia digital e dos dispositivos de processamento que podem conter a potencial evidência digital.

Esse processo também inclui uma atividade para priorizar a coleta das evidências baseada em sua volatilidade. Recomenda-se que a volatilidade dos dados seja identificada para garantir a correta ordem dos processos de coleta e aquisição para minimizar o dano à potencial evidência digital e para obter a melhor e mais completa evidência.

Adicionalmente, é oportuno que o processo identifique e considere a possibilidade de uma potencial evidência digital ocultada (por exemplo, um arquivo cancelado).

Com relação a identificação de mídias, o processo diz respeito tanto à identificação física (descrição, tipo, marca, número de série, fotografia etc.) quanto à identificação lógica, que, de norma, é realizada através do cálculo do valor (ou código) *hash*, utilizando funções quais MD5, SHA1 ou SHA2 (as mais comuns).

Com relação à preservação da evidência, essa diz respeito à proteção de sua integridade para garantia de sua utilidade e validade probatória. O processo de preservação envolve a guarda da evidência digital e do dispositivo digital que pode conter a evidência digital contra espoliação ou adulteração de qualquer tipo.

Recomenda-se que o processo de preservação seja iniciado e mantido durante o processo de manuseio da evidência digital, começando pela imediata identificação (física e lógica) do dispositivo digital que contém a potencial evidência digital, assim que se tem o primeiro contato com ele.

Recomenda-se, ainda, que não haja adulteração ou espoliação aos dados em si ou a quaisquer metadados associados a eles (por exemplo, registro de data e horário).

É necessário que seja possível demonstrar que a evidência não foi modificada, desde que ela foi coletada ou adquirida, ou de fornecer os fundamentos e ações documentadas se alterações inevitáveis foram feitas. No caso de mídias e arquivos, tal demonstração pode ser realizada a qualquer momento comparando o código *hash* calculado no momento da identificação inicial da evidência, com o código *hash* da evidência no momento da verificação, sendo certo que os dois códigos deverão ser idênticos.

É importante observar que, até em processos em curso, não é incomum encontrar situações onde os procedimentos e cuidados acima descritos foram completamente ou parcialmente desconsiderados pelas autoridades prepostas, sobretudo na fase investigativa.

É possível pensar que tal fenômeno seja consequência de falta de suficiente preparação técnica, equipamentos e competência no manuseio de evidências digitais, por parte de alguns agente públicos, mas pode haver também, às vezes, uma componente de descaso com o devido processo legal, possivelmente pela pressa de "mostrar serviço" e/ou de chegar a conclusões, sobretudo considerando que o conceito de preservação da cadeia de custódia não era, até o momento, explicitamente previsto em lei.

Seja o que for, isso já deu causa à invalidação de provas e anulação de processos no passado, quando a preservação da cadeia de custódia ainda era uma prática não explicitamente normatizada no Brasil, especialmente no que diz respeito às evidências digitais.

Agora, com o novo embasamento legal, deverá ser objeto de uma atenção cada vez maior por parte do Judiciário e passar a compor, de vez, o bojo dos procedimentos necessários para a legalidade e admissibilidade da prova digital (e não) no processo penal.

Date Created
18/06/2020