Lorenzo Parodi: Cadeia de custódia das provas digitais

Cada dia mais, as provas apresentadas pelos órgãos de persecução penal têm origem em material digital (arquivos ou dados) recebido de provedores de serviços de nuvem, ou outros sistemas digitais com armazenamento remoto (a exemplo de serviços de e-mail, redes sociais, sistemas de mensagens e comunicação etc.), em consequência de autorizações judiciais de quebra de sigilo de dados obtidas em

Não existe, até o momento, na legislação brasileira, uma tratação específica relativa aos procedimentos que devem ser adotados para este particular tipo de provas.

Existem, porém, normas gerais sobre a gestão das provas e de sua cadeia de custódia (artigos 158, 158-A a 158-F e 159 CPP, Portaria Senasp nº 82/2014, entre outros) e, de forma mais ampla, sobre a necessidade de garantir o acesso da defesa às provas íntegras e integrais (artigo 5º CF).

Existem também normas técnicas que tratam do assunto, notadamente a norma ABNT/ISO 27037, que trata especificamente de "identificação, coleta, aquisição e preservação de evidência digital". Importante, neste momento, observar que a ABNT, apesar de ser uma entidade independente, é o órgão brasileiro de normatização técnica reconhecido pelo Governo Federal e pelos organismos internacionais do setor.

Resumidamente, as normas aplicáveis a provas de tipo digital prescrevem os seguintes procedimentos:

1) Quando a infração deixar vestígios, será indispensável o exame de corpo de delito (extraído do artigo 158 CPP).
2) Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte (extraído do artigo 158-A CPP).
3) O agente público que reconhecer um elemento como de potencial interesse para a produção da prova pericial fica responsável por sua preservação (artigo 158-A, §2º CPP).
4) A coleta dos vestígios deverá ser realizada preferencialmente por perito oficial, que dará o encaminhamento necessário para a central de custódia, mesmo quando for necessária a realização de exames complementares (artigo 158-C CPP).
5) O vestígio deverá ser descrito detalhadamente, respeitando suas características e natureza e

armazenado e registrado de forma individualizada e inequívoca (extraído dos artigo 158-A CPP e artigos 3.1 e 3.5 da Portaria Senasp nº 82/2014).
6) Além de sua descrição genérica, a identificação segura de um vestígio ou prova digital e a sucessiva eventual verificação de sua integridade são normalmente implementadas através de funções hash, sendo as mais comuns as funções baseadas nos algoritmos MD5, SHA-1 e SHA-256 (extraído da norma ABNT/ISO 27037).
7) Os vestígios deverão ser protegidos de forma a evitar que se altere o estado das coisas, a garantir sua inviolabilidade e idoneidade e a preservar suas características, impedindo contaminação e garantindo o controle de sua posse (extraído dos artigos 158-B e 158-D CPP e artigo 1.5, §d da Portaria SENASP nº 82/2014).
8) O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior (artigo 159 CPP).

É, portanto, possível definir qual seria um procedimento correto para tratamento e custódia da prova digital oriunda de nuvem e sistemas afins, no processo penal, de acordo com as normas vigentes no Brasil, quando não por prescrição explícita, no mínimo por analogia.

Importante também notar que, via de regra, os provedores, quando do cumprimento da determinação judicial com a entrega dos dados e arquivos, não informam os códigos hash do material fornecido, cabendo, portanto, ao Juízo solicitar preliminarmente que, neste caso, em obséquio ao artigo 158-C CPP, o material seja entregue ao órgão oficial de perícia, para que sejam adotados os necessários procedimentos de custódia, especialmente o cálculo da função de hash, de forma a garantir a integridade futura de quanto recebido.

Vejamos como, na atualidade, os provedores de serviços normalmente fornecem os dados presentes em seus sistemas, quando recebem ofício com autorização judicial encaminhado pela autoridade que investiga.

Os principais provedores de serviços que mantêm dados em nuvem (ou de outra forma armazenados remotamente) que são frequentemente fonte de provas utilizadas em ações penais são Google (Google Drive e Gmail), Apple (ICloud), Microsoft (OneDrive e Outlook/Hotmail/Skype) e Facebook.

De forma geral os dados solicitados aos provedores são normalmente fornecidos por estes utilizando uma das seguintes formas: a) entrega de uma mídia (pen drive ou outra), contendo os arquivos extraídos da nuvem ou sistema remoto b) fornecimento dos arquivos como anexo a um e-mail c) fornecimento de um link para baixar os arquivos.

Adicionalmente os dados ou arquivos podem ser fornecidos sem qualquer tipo de compressão (ou seja, livremente e diretamente acessíveis), armazenados em uma base de dados (com ou sem restrições para edição) ou planilha, compactados em algum arquivo, mas sem criptografia nem restrições, compactados e criptografados de várias formas, eventualmente até com restrição para alterações (nos limites do possível, pois, normalmente, trata-se de restrições que podem ser superadas ou contornadas).

Os principais provedores acima mencionados, normalmente fornecem os dados e arquivos nos seguintes formatos:

– Apple / ICloud: utiliza normalmente o formato criptográfico "GPG", frequentemente aplicado a conjuntos de pastas e arquivos já compactados no formato "ZIP".
– Google Drive/Gmail: utiliza normalmente o formato ZIP, sendo que diversos arquivos (sobretudo relatórios e listagens) podem ser fornecidos no formato PDF ou no formato XLSX.
– Microsoft OneDrive /Outlook/Skype: utiliza normalmente o formato ZIP com criptografia protegida por senha. Por vezes pode informar o código hash do material fornecido.

Arquivos em todos estes formatos, quando não adequadamente identificados e custodiados, podem ser objeto de consistentes adulterações que podem facilmente ser realizadas de forma rápida e indetectável.

Podem ser adicionados, modificados, substituídos ou eliminados arquivos e dados, sem deixar qualquer rastro.

Pode até ser integralmente substituído o arquivo (GPG, ZIP ou outros, mesmo quando criptografado) recebido dos provedores por outro, diferente no conteúdo, mas com o mesmo nome, o mesmo sistema de criptografia ou compactação e a mesma senha de acesso.

Em suma, na ausência de uma identificação segura, através de códigos hash, do material digital fornecido, que pode ser informada pelos provedores na origem ou realizada pelo órgão oficial de perícia imediatamente quando do recebimento, provas deste tipo perderão integralmente e de forma irrecuperável sua confiabilidade e higidez e, por consequência, não terão condição de serem submetidas ao contraditório judicial ou de serem utilizadas para embasar uma tese acusatória ou uma medida cautelar.

Por tudo isso entendo que, de acordo com as normas em vigor, o procedimento correto, para garantir a custódia e integridade dos dados e arquivos recebidos, deva ser o seguinte:

a) A autoridade que investiga solicita a quebra de sigilo de dados ao Juiz, que defere e intima o provedor a entregar, diretamente ao órgão oficial de perícia, determinados dados e arquivos armazenados em seus sistemas.
b) O provedor envia ao órgão oficial de perícia os dados e arquivos solicitados no formato e pelos meios que normalmente utiliza.
c) O órgão oficial de perícia recebe o material do provedor e, quando o provedor não tiver indicado, em suas comunicações oficiais, o código hash que identifica tal material, imediatamente realiza os procedimentos de custódia necessários, entre os quais o imediato cálculo e registro em relatório oficial dos códigos hash de todo o material digital recebido.
d) O órgão oficial de perícia, uma vez realizados os procedimentos para garantir a custódia e integridade do material digital recebido, poderá realizar uma cópia forense de tal material e entregar à autoridade investigadora para a realização das análises que esta julgar necessárias.

Entendo que, no caso de provas recebidas de nuvens e sistemas remotos em geral, qualquer outro

procedimento que não compreenda, no mínimo, o envio dos códigos hash por parte dos provedores ou o imediato cálculo dos códigos hash do material recebido (procedimento este indicado como padrão também pela mencionada norma ABNT/ISO 27037) por parte do órgão oficial de perícia (conforme previsto pelos artigos 158-A a 158-D e 159 CPP), não ostentará a necessária confiabilidade e segurança quanto à originalidade, autenticidade, integridade e integralidade da prova, para posterior análise por parte da defesa e, por isso, ferirá mortalmente e de forma irrecuperável, entre outros, os direitos ao contraditório, ampla defesa e paridade de armas.

Considerando a natureza e as peculiaridades deste tipo de provas, facilmente adulteráveis de forma rápida e indetectável, o recebimento do material diretamente por parte da autoridade investigadora, sem a participação do órgão oficial de perícia (que identifique e custodie o material recebido no exato momento de seu recebimento), e quando não acompanhado por identificação através de códigos hash fornecidos diretamente pelo provedor em suas comunicações oficiais, ensejará, para os efeitos práticos, uma situação em tudo equivalente aos mais graves casos de quebra da cadeia de custódia.

Por fim, vale mencionar que os procedimentos acima descritos parecem ser os únicos que, no tratamento das provas objeto deste artigo, respeitam os Princípios Administrativos descritos no artigo 37 CF, quais sejam: Legalidade, Impessoalidade, Moralidade, Publicidade e Eficiência.

Date Created
10/04/2022