LAUDO TÉCNICO

▶ 1 - Premissas

O abaixo assinado Lorenzo Parodi, perito em forense digital, fraudes e falsificações, inscrito no rol dos peritos da Justiça Federal, do TJSP e de diversos outros Tribunais Estaduais, e atuante nestes órgãos na qualidade de Perito Judicial nas áreas acima, membro das comissões de estudos sobre perícias forenses da OAB-SP e da OAB-RJ, professor no curso de pós-graduação em "Perícia e Crimes Digitais" da faculdade Verbo Jurídico e em diversos outros cursos de nível superior a exemplo do curso de "Direito Processual Penal" da EMERJ (Escola da Magistratura do RJ), autor dos livros "Manual das Fraudes" (1ª e 2ª edição, 2005 e 2008) e "Falsificação de Documentos em Processos Eletrônicos" (2018), pela Editora Brasport, e do livro "Perícia Defensiva em Provas Digitais no Processo Penal" (2024), pela Editora Revista dos Tribunais, além de numerosas matérias e artigos de cunho acadêmico publicados, entre outros, pelos reconhecidos portais *Conjur, Migalhas, Âmbito Jurídico, e Administradores*, foi contratado por Marcos Antonio Alle Teixeira, representado por seu advogado Dr. Igor Luiz Batista de Carvalho, OAB/RJ nº 157.242, para analisar documentos e arquivos digitais supostamente extraídos de aparelho celular apreendido e utilizados como provas no âmbito da ação penal nº 0170186-48.2023.8.19.0001, em tramite perante o Juízo da 1ª Vara Criminal Especializada da Comarca da Capital do Rio de Janeiro (RJ).

▶ 2 - Material Analisado e Escopo

Neste trabalho será analisado tão somente o material que diz respeito ao aparelho celular alegadamente objeto de Apreensão em 10/05/2022 (Auto de Apreensão nº 079776-1016/2022 - Procedimento nº 016-08730/2022) e atribuído ao Sr. Nelson Gomes Pereira Junior.

Neste trabalho foram analisadas as seguintes classes de documentos:

1) Autos, incluindo especialmente os registros e documentos relativos a apreensões e sucessivos procedimentos realizados no material apreendido.
2) Material digital fornecido pela Vara competente em um HDs e sucessivamente em um pendrive, como sendo a integralidade do material digital juntado aos Autos pelo Estado, contendo, entre outros, o suposto material digital extraído do aparelho celular acima mencionado.

pericias@ibracaf.com.br · 011-99271.2064 · www.parodi.in

O escopo deste trabalho limita-se à análise dos documentos presentes nos autos e do material digital fornecido, visando verificar a licitude, higidez, admissibilidade, integridade e integralidade de tal material e a aderência dos procedimentos adotados às Leis e demais normas vigentes.

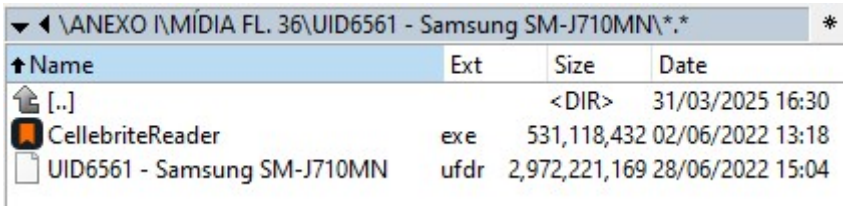


Fig. 01

Os arquivos digitais analisados neste trabalho são aqueles alegadamente extraídos do aparelho celular Samsung SM-J710MN, sendo em tese o aparelho apreendido em 10/05/2022, conforme Auto de Apreensão nº 079776-1016/2022, e atribuído ao mencionado Sr. Nelson, conforme entregues pela Vara no formato UFDR (com dimensão total de 2.972.221.169 Bytes), em uma pasta do último pendrive disponibilizado à defesa (Fig. 01).
Para acessar os arquivos e dados extraídos do aparelho celular, foi utilizado o software “Cellebrite Reader” fornecido na mesma mídia.

Esclareço que o formato UFDR, nada mais é que um formato de arquivos, proprietário do sistema Cellebrite, para a disponibilização (total ou parcial/seletiva, a depender de como for gerado tal arquivo UFDR) do material digital extraído, que, por ser indexado, permite a realização facilitada de pesquisas, buscas e, mais em geral, da visualização organizada de tal material.

▶ 3 - Análises e Resultados

Destarte é necessário observar que, de acordo com a documentação encartada e conforme será melhor detalhado a seguir, em relação ao aparelho celular em foco, não foi adotado nenhum dos procedimentos de custódia previstos pelos Arts. 158-A a 158-F do CPP, em vigor à época.

Adicionalmente a suposta extração de dados do mencionado aparelho celular (na realidade uma extração espúria, como veremos), foi realizada de forma diferente de quanto previsto pelas normas e melhores práticas em vigor (Art. 159 e Art. 158-D do CPP, POP/2013 - Procedimento Operacional Padrão da SENASP etc.).

Um rápido resumo do alegado histórico do aparelho celular em foco, de acordo com a documentação existente nos autos, é o seguinte:

1) No dia 10/05/2024, as 09:13 horas, no âmbito de flagrante, foi formalmente lavrada a apreensão do suposto aparelho celular acima descrito, atribuído ao Sr. Nelson Gomes Pereira Junior, que na realidade já tinha sido apreendido por policiais militares por volta da 6:00 horas.

2) De acordo com as informações presentes no Auto de Apreensão (Fig. 02), o aparelho celular não foi identificado de qualquer forma minimamente confiável (não há sequer a marca e/ou modelo do aparelho, não é mencionada a cor e somente é indicado um suposto IMEI que não corresponde plenamente aquele posteriormente indicado no momento da extração de dados) e, sobretudo, foi removido do local da apreensão (uma via pública, próximo a residência de um investigado - Fig. 03[1]) sem a prévia liberação por parte de perito oficial responsável, infringindo a expressa proibição do Art. 158-C, § 2º do CPP.

GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DE POLÍCIA CIVIL

016a.Delegacia de Polícia
Praça Desemb. Araújo Jorge, S/N, Barra Da Tijuca, Rio De Janeiro - RJ, CEP: 22611-220
TEL.: (21) 2333-6364

245
Fl.

AUTO DE APREENSÃO

Controle Int.: 079776-1016/2022 **Procedimento: 016-08730/2022**

Data: 10/05/2022 às 9:13 Horas

APRESENTANTE ERIC ROSA SCARPINE - 81384 - PMERJ
GSI/MPRJ

Primeira Testemunha

JALDEMIR BARBOSA DE LIMA - PMERJ-66946
GSI/MPRJ

Especificação do Material:

Outros Bens:

*Telefone Celular: 1 Unidade(s) IMEI 2 - 351972086937823O1

Nada mais havendo, é encerrado o presente que vai por todos assinado.

ALEX ADALBERON BRAGA DA SILVEIRA
Inspetor de Polícia - 872.323-1
Assinado por ordem do(a) RODRIGO FREITAS DE

ALEX ADALBERON BRAGA DA SILVEIRA
Inspetor de Polícia - 872.323-1

Fig. 02

[1] Descrição da apreensão extraída da decisão judicial exarada em data 14/10/2022

pericias@ibracaf.com.br · 011-99271.2064 · www.parodi.in

Segundo consta nos autos, quando do cumprimento da diligência de busca e apreensão ("Operação Calígula"), ocorrida no dia 10 de maio de 2022, no endereço residencial de ROGÉRIO DE ANDRADE, encontrava-se, à espera das equipes policiais, ainda em via pública, às 06:00 horas da manhã, o nacional NELSON GOMES PEREIRA JUNIOR, que se apresentou como pessoa indicada pelo advogado JOÃO MAIA (patrono constituído por ROGÉRIO DE ANDRADE), como responsável pelo acompanhamento da diligência.

Ocorre que a diligência em questão era sigilosa.

Além disso, conforme afirmado pelo Parquet, o nacional NELSON estava em atitude semelhante aos seguranças de ROGÉRIO DE ANDRADE, inclusive demonstrando possuir prévia ciência sobre a deflagração da "Operação Calígula", até porque estava aguardando as equipes no local das buscas às 06:00 h.

Assim, as equipes que cumpriam a ordem de busca e apreensão entenderam prudente, apresentá-lo à autoridade policial, juntamente com seu aparelho telefônico, objeto de apreensão (Auto de Apreensão nº 079776-1016/2022).

Fig. 03

3) Não foi encontrado nos autos um termo de apreensão redigido no local da apreensão, mas tão somente o Auto de Apreensão acima mencionado, redigido na delegacia (Fig. 02) horas mais tarde.
   Em tal documento não consta o acondicionamento em recipiente individualizador apropriado nem a aposição de um lacre no mencionado aparelho celular apreendido, conforme previsto pelo Arts. 158-B e 158-D do CPP.

4) O aparelho apreendido <u>não</u> foi encaminhado à Central de Custódia, junto ao competente Instituto de Criminalística (Art. 158-C, caput, do CPP). Em vez disso, na mesma data de 10/05/2022, em nítida violação às regras de custódia, foi requisitado pelo Ministério Público e a ele encaminhado (Fig. 04), sempre sem lacre e acondicionamento próprio.

Despacho

Controle Int.: 080086-1016/2022

Data: 10/05/2022 às 13:53 Procedimento: 016-08730/2022

Despacho Nº: 1º Despacho de RO

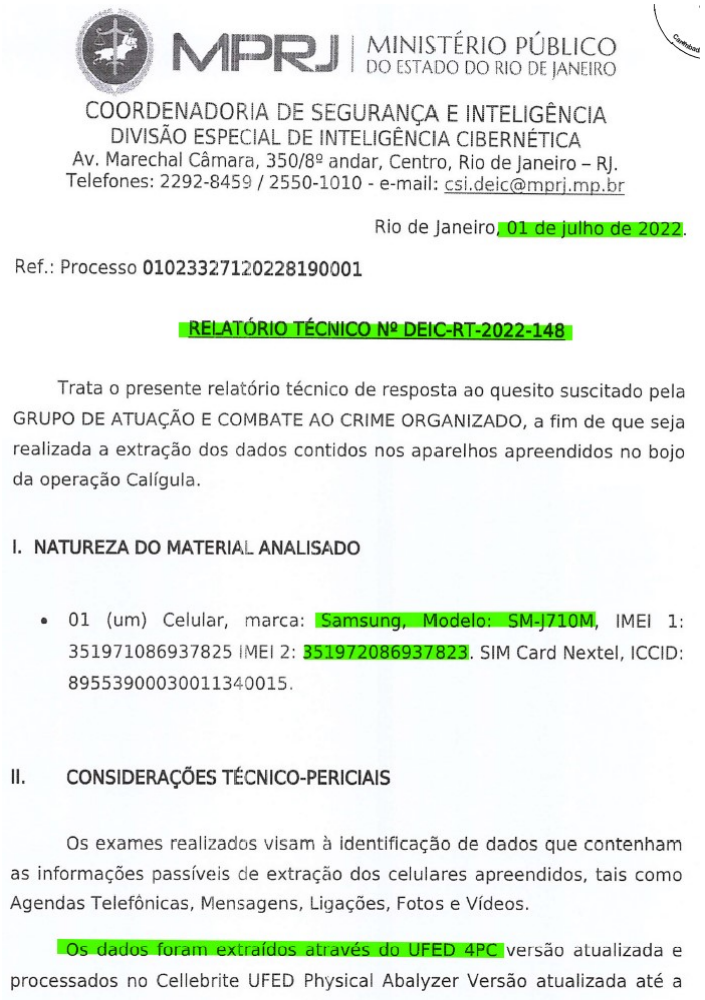
Categoria: RO

Status: Enc.Outros Órgãos

Considerando que o telefone apreendido foi requisitado pelo MP e devidamente encaminhado, não vislumbro outra medida que não seja a remessa do proprio procedimento ao MP a fim de que o mesmo prossiga na investigação

Fig. 04

5) Em 01/07/2022 (50 dias após a apreensão, como o celular sempre a mercê de quem quisesse modificar seu conteúdo, pois sem lacre), de acordo com o "Relatório Técnico nº DEIC-RT-2022-148" do próprio Ministério Público (Fig. 05), foi realizada extração de dados espúria (pois realizada de forma contrária a quanto previsto pelas normas aplicáveis), pelos próprios assistente técnicos da acusação (potencialmente interessados em comprovar suas teses acusatórias), de fato prejudicando definitivamente a já inexistente integridade e confiabilidade de tal evidência. Cabe observar que os assistentes técnicos da acusação, além de não terem competência legal para realizar tal procedimento e de não terem qualquer isenção nem autonomia, por serem diretamente subordinados ao MP, não podem de forma alguma serem equiparado aos peritos digitais, especialmente em força da Lei 12.030/2009. Neste sentido, inclusive, já se manifestou o STJ[2].



MPRJ | MINISTÉRIO PÚBLICO DO ESTADO DO RIO DE JANEIRO

COORDENADORIA DE SEGURANÇA E INTELIGÊNCIA
DIVISÃO ESPECIAL DE INTELIGÊNCIA CIBERNÉTICA
Av. Marechal Câmara, 350/8º andar, Centro, Rio de Janeiro – RJ.
Telefones: 2292-8459 / 2550-1010 - e-mail: csi.deic@mprj.mp.br

Rio de Janeiro, 01 de julho de 2022.

Ref.: Processo 01023327120228190001

RELATÓRIO TÉCNICO Nº DEIC-RT-2022-148

Trata o presente relatório técnico de resposta ao quesito suscitado pela GRUPO DE ATUAÇÃO E COMBATE AO CRIME ORGANIZADO, a fim de que seja realizada a extração dos dados contidos nos aparelhos apreendidos no bojo da operação Calígula.

I. NATUREZA DO MATERIAL ANALISADO

- 01 (um) Celular, marca: Samsung, Modelo: SM-J710M, IMEI 1: 351971086937825 IMEI 2: 351972086937823. SIM Card Nextel, ICCID: 89553900030011340015.

II. CONSIDERAÇÕES TÉCNICO-PERICIAIS

Os exames realizados visam à identificação de dados que contenham as informações passíveis de extração dos celulares apreendidos, tais como Agendas Telefônicas, Mensagens, Ligações, Fotos e Vídeos.

Os dados foram extraídos através do UFED 4PC versão atualizada e processados no Cellebrite UFED Physical Abalyzer Versão atualizada até a

Fig. 05

[2] Acordão no HC nº 154.093/RJ, relator Min. Jorge Mussi, julgado em 09/11/2010.

6) Em 27/09/2022 (mais de 5 meses após a apreensão e 4 meses após a extração de dados espúria realizada pelo próprio Ministério Público) o MP apresentou ao Juízo competente um requerimento especifico (Fig. 06) para que fosse autorizada, entre outros, a quebra de sigilo de dados do aparelho celular em foco, especificando se tratar do aparelho apreendido no Procedimento nº 016-08730/2022, aquele mesmo do Auto de Apreensão do aparelho em foco, reproduzido na Fig. 02.
Importante lembrar que em 01/07/2022 já tinha sido emitido um documento do próprio MP (Fig. 05) informando a realização de tal extração de dados, obviamente sem autorização judicial, pois ocorrida 4 meses antes do requerimento do MP ao Juízo!

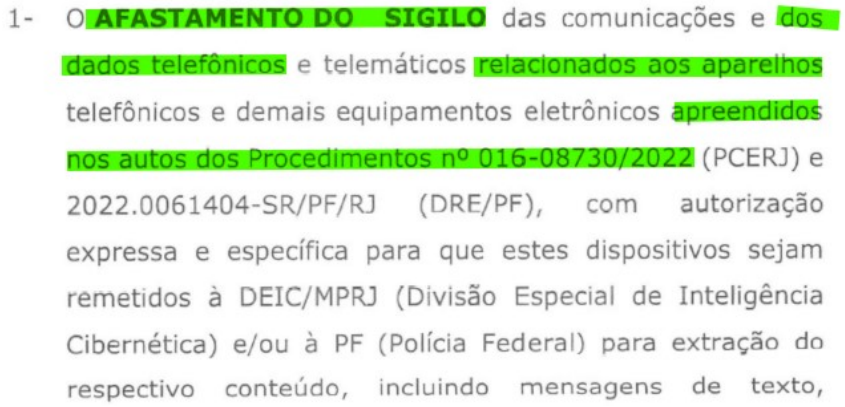

1- O **AFASTAMENTO DO SIGILO** das comunicações e dos dados telefônicos e telemáticos relacionados aos aparelhos telefônicos e demais equipamentos eletrônicos apreendidos nos autos dos Procedimentos nº 016-08730/2022 (PCERJ) e 2022.0061404-SR/PF/RJ (DRE/PF), com autorização expressa e específica para que estes dispositivos sejam remetidos à DEIC/MPRJ (Divisão Especial de Inteligência Cibernética) e/ou à PF (Polícia Federal) para extração do respectivo conteúdo, incluindo mensagens de texto,

Fig. 06

7) Em 14/10/2022 o Juízo competente, evidentemente ainda ignorando que o MP já há 4 meses tinha realizado a invasão e quebra de sigilo de dados de tal aparelho, deferiu a autorização (de fato "póstuma") para quebra de sigilo e extração dos dados presentes no aparelho celular em foco. Cabe sublinhar dois pontos de tal decisão:
   A) A decisão menciona a necessariedade da observância da cadeia de custódia, a qual, porém, nunca tinha sequer sido iniciada, sendo, portanto, inexistente.
   B) A decisão é passível de questionamento pois não se coaduna com as normas em vigor, notadamente por determinar, sem qualquer justificativa plausível, que o aparelho fosse encaminhado ao MP para realizar a extração de dados, isso enquanto o Art. 159 do CPP determina que os procedimento de análise dos vestígios são de competência dos perito oficiais, o Art. 158-D do CPP determina que o lacre (de fato inexistente no caso em foco) somente pode ser aberto pelo perito encarregado da análise e, motivadamente, por pessoa

pericias@ibracaf.com.br · 011-99271.2064 · www.parodi.in

autorizada e o POP/2013[3] 3.2 (Procedimento Operacional Padrão, publicado pela SENASP – Órgão do Ministério da Justiça) em seu artigo 4.2 define a "Extração de Dados" como um dos procedimentos de análise contemplados e no Art. 5º (Pag. 96 do POP), determina que "*A evidência digital deve ser examinada apenas por peritos criminais com treinamento específico para esse propósito.*", sendo que perito criminal oficial, por obvio, é tão somente aquele descrito na Lei 12.030/2009[4], como sendo profissional concursado no cargo, lotando em Instituto de Criminalística e gozando de autonomia técnica e funcional (aspectos fundamentais, pelas razões que veremos mais a frente).

Vejamos tudo quanto acima mais em detalhes e por partes.

A apreensão do aparelho celular ocorreu, no dia 10/05/2022, no âmbito de uma operação de busca e apreensão, ou seja, uma operação previamente planejada, que previa a possível (ou até provável) apreensão de vestígios e outros itens relacionados a supostos crimes.

Por esta razão, em observância aos Arts. 158-A a 158-F do CPP, e em especial ao Art. 158-C de tal código processual, deveria ter sido prevista e planejada a participação de perito oficial, que tem exclusiva competência para autorizar a "remoção" do local em que for encontrado, de qualquer item apreendido, além de ter a competência preferencial para a realização do simples ato da "coleta".

Cabe sublinhar que, de acordo com o Art. 158-B, inciso IV do CPP, a "coleta" representa tão somente o ato de recolher o item, ato bem diferente da "remoção", descrita no § 2º do Art. 158-C e no inciso VI do Art. 158-B, como "transporte" ou seja, remoção de um local para outro.

Apesar de tal planejamento prévio e previsão legal, ao que tudo indica, não foi solicitada a presença de nenhum perito oficial para que participasse da execução do mandado de busca e apreensão, numa omissão voluntária.

Ademais, nem mesmo quando foi apreendido o aparelho celular do Sr. Nelson foi solicitada a presença do competente perito oficial responsável, para que verificasse os procedimentos adotados e liberasse a "remoção" de tal item, com as devidas cautelas.

[3] https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf

[4] https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12030.htm

Como uma das consequências de quanto acima (ausência de perito oficial quando da apreensão), não foi redigido nenhum Termo de Apreensão do aparelho em foco no real local de sua apreensão (a via pública na proximidade do local de execução do mandado de busca e apreensão) mas tão somente tempos depois, quando da chegada na delegacia, não sendo possível averiguar as manipulações indevidas realizada em tal celular (apreendido sem qualquer cuidado de preservação) eventualmente ocorridas no período de tempo entre a apreensão e a apresentação na delegacia.

Além disso o aparelho celular apreendido foi removido do local da apreensão sem a previa liberação do perito oficial responsável, em nítido e frontal descumprimento da explícita proibição prevista no parágrafo 2º do Art. 158-C do CPP.

Isso significa que o Ato Administrativo da Apreensão, por ter sido realizado de forma frontalmente contrária as previsões legais (no caso, desrespeitando uma explícita proibição), não atente ao fundamental requisito da "legalidade", fazendo com que tal Ato Administrativo (e, por consequência, toda a Apreensão e atos seguintes, dela derivados) deva ser considerado inválido e nulo de direito, com as consequências do caso.

Ademais, nem na delegacia o aparelho celular apreendido foi objeto do acondicionamento individualizados e da aposição do lacre previstos explicitamente pelo Art. 158-D do CPP. Cabe observar que tal aparelho, além de não ter sido acondicionado nem lacrado no momento da apreensão, nem sequer foi identificado de forma minimamente confiável sendo que, no Auto de Apreensão, é descrito tão somente como "Telefone Celular" (Fig. 02), com indicação de um número de IMEI (35197208693782301) que nem sequer bate plenamente com o IMEI mais tarde encontrado (351971086937825), quando da realização de extração de dados espúria (Fig. 07 – detalhe B).

Com isso, não é possível saber ao certo se o celular que, posteriormente, foi objeto de extração de dados espúria, foi o mesmo que tinha sido apreendido ou outro, eventualmente preparado para se coadunar com determinadas teses acusatórias. Isso porque o número de IMEI não é um meio seguro para identificação de aparelhos celulares, por ser perfeitamente possível (na ausência de custódia, como no caso em foco) editar tal número para se coadunar a qualquer outro[5].

[5] https://olhardigital.com.br/2018/02/23/seguranca/maquina-troca-imei-de-celulares-e-faz-aparelhos-bloqueados-voltarem-a-funcionar/

Isso significa que, na prática, qualquer celular, de qualquer modelo, poderia ter sido substituído ao aparelho efetivamente apreendido, em função da total ausência de custódia (uso do lacre, Art. 158-D, §1º), agravada por uma identificação absolutamente insuficiente.

Adicionalmente, ao que se depreende dos autos, o aparelho apreendido não foi encaminhado a competente Central de Custódia, conforme previsto pelo Art. 158-C, caput, do CPP, mas sim indevidamente solicitado e encaminhado ao Ministério Público (Fig. 04), sempre totalmente deslacrado, ou seja, desprotegido e à mercê de quem quisesse adulterar seu conteúdo.

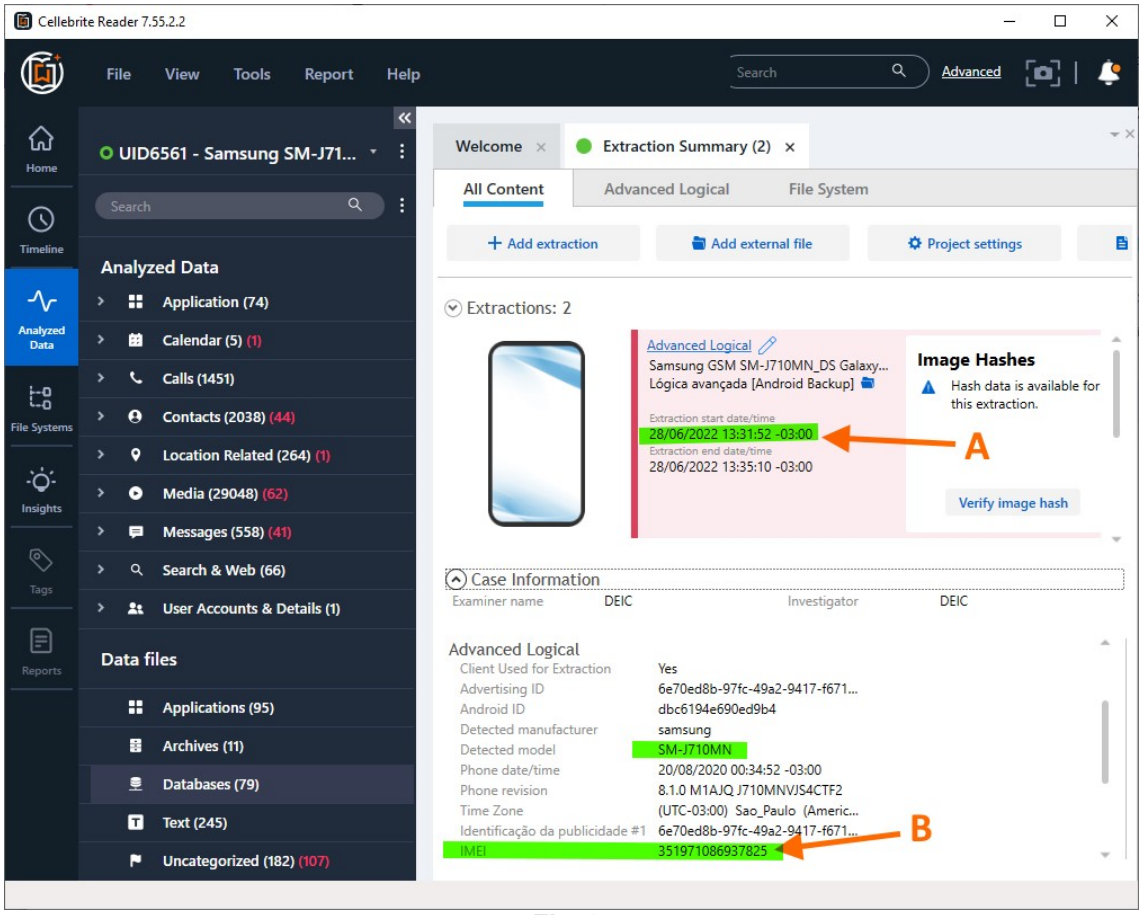


Fig. 07

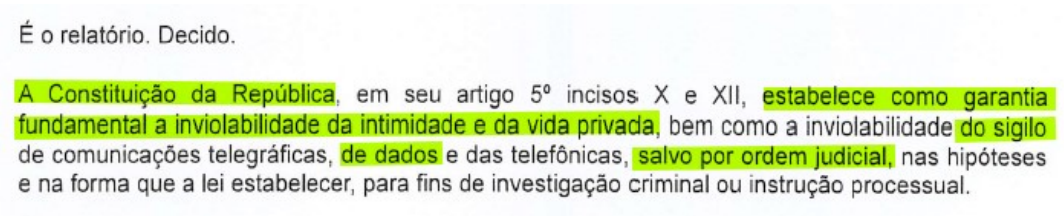
Em 01/07/2022, de acordo com o documento da Fig. 05 (mas na realidade alguns dias antes, em 28/06/2022, conforme se depreende acessando o arquivo UFDR fornecido nos autos – Fig. 07, detalhe A), foi realizada uma extração de dados espúria, pois não realizada por peritos oficiais, mas sim pelos assistentes técnicos da acusação (Ministério Público), contrariamente a quanto previsto pelo Art. 159 do CPP e pelo já mencionado POP/2013 da SENASP (Órgão do Ministério da Justiça).

Evidente o conflito de interesses de tais assistentes técnicos de uma parte (a acusação), pois potencialmente interessados em confirmar determinadas teses acusatórias.

Ademais, tal extração de dados, que constitui a quebra do sigilo de dados eletrônicos armazenados no aparelho, foi realizada sem a previa autorização judicial, e, portanto, infringindo frontalmente o Art. 5º (incisos X, XII e LXXIX) da Constituição Federal.

Com efeito, somente 2 meses mais tarde, em 27/09/2022, o MP solicitou o deferimento judicial da quebra de sigilo de dados, e somente em 14/10/2022 o Juízo competente deferiu tal autorização, fazendo com que a extração ocorrida em 28/06/2022, seja nitidamente eivada de ilicitude tanto por não ter sido realizada por que tinha a competência legal para tanto (perito oficiais), quanto pode ter sido realizada sem a necessária prévia autorização judicial de quebra do sigilo de dados eletrônicos e em item não preservado através dos devidos procedimentos de custódia.

O próprio Juízo, em sua decisão, corretamente lembrou a inviolabilidade do sigilo de comunicações e dados, salvo por ordem judicial prévia (Fig. 08).



É o relatório. Decido.

A Constituição da República, em seu artigo 5º incisos X e XII, estabelece como garantia fundamental a inviolabilidade da intimidade e da vida privada, bem como a inviolabilidade do sigilo de comunicações telegráficas, de dados e das telefônicas, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer, para fins de investigação criminal ou instrução processual.

Fig. 08

Importante também salientar que a própria realização da suposta extração de dados por parte dos mesmos agentes que conduzem a investigação (e por isso têm um nítido conflito de interesses entre preservar a integridade da prova e conseguir comprovar suas próprias teses acusatórias), por si só, independentemente do uso ou menos de lacres, constituiria uma quebra da cadeia de custódia (se algum procedimento de custódia tivesse existido) e faria com que todo este material deixasse de ser confiável, de forma irreversível, em vista do fato que, na ausência de adequado e rígidos procedimentos de custódia, é perfeitamente possível adulterar o conteúdo do aparelho celular, inclusive de forma indetectável, como será melhor explicado mais à frente.

Como já mencionado, o alegado material extraído digital extraído do aparelho celular em foco foi disponibilizado no formato compactado UFDR (padrão do sistema Cellebrite).

Analisando tal material digital (através da extração integral, ou "*dump*", do conteúdo disponibilizado para uma pasta, onde resultou o total de 29.883 arquivos), foi possível verificar que o mesmo foi objeto de manipulações indevidas após a data da apreensão e antes da alegada data da mencionada extração de dados espúria, pois realizada por assistentes técnicos da parte acusação.

Quando acima se deduz e comprova pela existência, no mencionado material digital fornecidos e alegadamente extraído do aparelho apreendido, de diversos arquivos que apresentam como data de última modificação uma data posterior ao dia 10/05/2022, data da apreensão do aparelho (Fig. 09, detalhes C).

Analisando os dados em questão pelo próprio software Cellebrite se confirma ainda que o banco de dados do Aplicativo WhatsApp (que armazena as mensagens enviadas e recebidas), denominado "*msgstore.db*", apresenta data de última modificação no dia 15/05/2022 (Fig. 09, detalhe A e Fig. 10), ou seja, 5 dias após a apreensão do aparelho, enquanto este se encontrava, sem lacre nem custódia, aparentemente nas mãos do Ministério Público (Fig. 04).

Seja o que for que foi modificado em tal arquivo de banco de dados (inserção, exclusão ou edição/modificação), resta o fato que o mesmo certamente não se encontra mais integro e nas condições em que se encontrava quando da apreensão do aparelho celular, em 10/05/2022.

Cabe ainda observar que existem em tal material diversos outros arquivos relacionados ao aplicativo WhatsApp que apresentam data de criação ou última modificação posterior à data da apreensão.

Em especial há arquivos de "log" (que registram o uso do aplicativo), nas datas de 12, 13,14 e 15 de maio de 2022, significando que ao menos nestas datas o aparelho foi manipulado e, especialmente, os dados do aplicativo WhatsApp foram acessados e possivelmente manipulados (Fig. 09, detalhes B).

Há também o arquivo da agenda de contatos do aplicativo WhatsApp (arquivo de banco de dados denominado "*wa.db*"), que apresenta a data de última modificação no dia 14/05/2022 (Fig. 09, detalhe D e Fig. 10).

Por outro lado, foi observada a estranha ausência, entre os dados extraídos, do arquivo de banco de dados da agenda de contatos do celular (arquivo denominado "*contacts.db*"), que pode ser explicada somente de duas maneiras:

A) Tal arquivo foi removido/omitido por quem realizou a extração ou,

B) Neste aparelho ninguém nunca registrou um contato sequer na agenda de contatos, nunca tendo sido tal agenda criada.

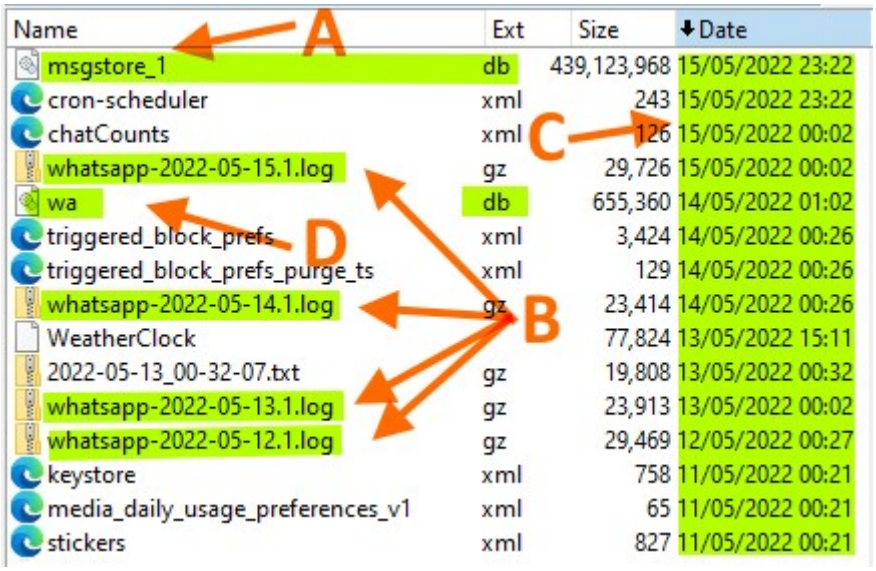


Fig. 09

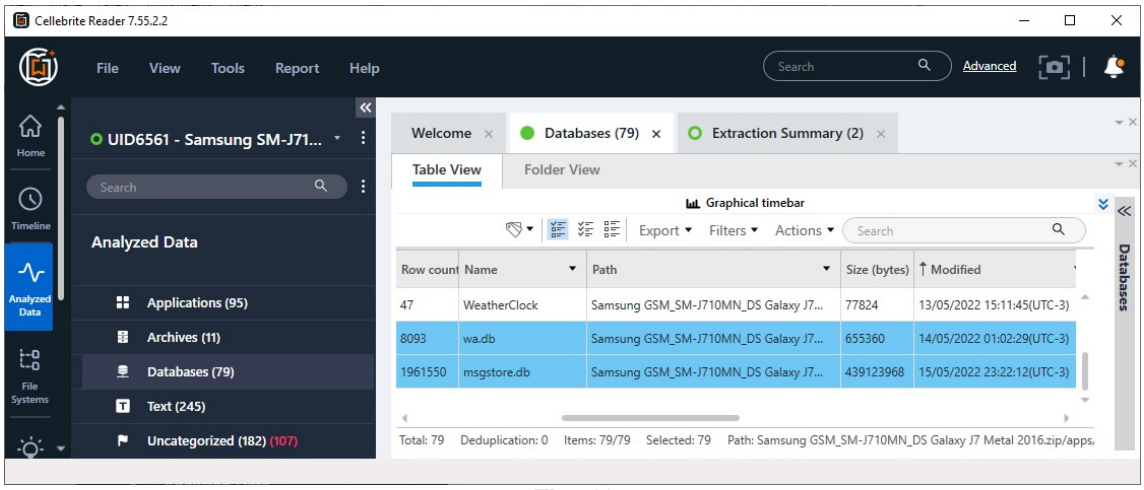


Fig. 10

Cabe informar que os arquivos de banco de dados utilizados majoritariamente nos aparelhos celulares (entre os quais certamente os bancos de dados do aplicativo WhatsApp e das agendas de contatos, entre muitos outros), utilizam o formato SQLITE, e, na ausência de apropriados procedimentos de custódia (como no caso em foco), podem ser facilmente editados (se entendendo por isso inclusão, exclusão e modificação de registros de qualquer tipo) até com uso de ferramentas gratuitas.

Na prática, os relevos acima demonstram não somente que não foram adotados os necessários e devidos procedimentos de custódia em relação ao aparelho apreendido em foco, mas que tal falta de custódia foi efetivamente aproveitada por quem ficou de posse do aparelho, sem custódia adequada (ou seja, livremente acessível), para manipular indevidamente o aparelho celular em foco, sem prévia autorização judicial, inclusive quebrando a integridade de seu conteúdo, que foi modificado em datas posteriores à apreensão.

É até perfeitamente possível que tenha sido adulterado tal conteúdo de forma ainda mais abrangente que aquela já demonstrada acima, o que não se pode demonstrar (assim como não se pode demonstrar o contrário) justamente em função da não adoção dos procedimentos de custódia, em conjunto com as características das evidências digitais, que, na ausência de custódia, podem ser adulteradas de forma indetectável.

Feitas as análises e observações acima, em relação ao aparelho em exame, se faz necessário analisar a situação geral deste conjunto probatório, sua validade, fiabilidade e admissibilidade, à luz das Leis e demais normas aplicáveis e das considerações técnicas cabíveis.

Iniciaremos descrevendo qual seria o procedimento correto para apreensão e custódia de um aparelho celular, de acordo com as leis e demais normas vigentes e com as melhores práticas periciais, o que inclui os Arts. 158-A a 158-F do CPP, o POP/2013 - Procedimento Operacional Padrão, publicado em 2013 pela SENASP, órgão do Ministério da Justiça, e a Portaria nº 82/2014[6] da mesma SENASP.

Os corretos procedimentos de apreensão e custódia deveriam ter sido, resumidamente, os seguintes:

1) Coleta do aparelho apreendido por parte de peritos oficiais (em casos excepcionais o simples ato da coleta, diferente do ato da remoção, pode ser realizado por outro agente), com imediato acondicionamento individualizador, isolamento (desligando o aparelho ou através do uso de gaiola de Faraday), aposição de lacre por parte do perito responsável no próprio local e momento da apreensão (Arts. 158-C e 158-D do CPP e Arts. 3.1, 3.2, 3.3, 3.4 da mencionada portaria nº 82 da SENASP).

6 https://pesquisa.in.gov.br/imprensa/servlet/INPDFViewer?jornal=1&pagina=42&data=18/07/2014&captchafield=firstAccess

2) Lavra de Auto ou Termo de Apreensão circunstanciado (Art. 245, § 7º do CPP), contextual ao momento da apreensão, com descrição do item apreendido, do acondicionamento realizado e do lacre aposto, além de identificação dos presentes, ou seja, as testemunhas presenciais, os agentes e o perito oficial responsável (ex vi Art. 158-C, § 2º do CPP).
Neste documento deverão também constar, entre outras, as informações previstas no Art. 3.5 da mencionada Portaria nº 82 da SENASP.

3) Após liberação, documentada, por parte do perito oficial responsável (ex vi Art. 6º, inciso II do CPP, e, mais detalhadamente, Art. 158-C, § 2º do CPP), remoção/transporte do item apreendido para seu imediato encaminhamento à Central de Custódia junto ao competente Instituto de Criminalística.

4) Após autorização judicial para quebra de sigilo de dados eletrônicos, realização da extração dos dados do aparelho celular, exclusivamente por parte de perito oficial (Art. 159 do CPP e POP/2013, 3.2 da SENASP), com sucessivo cálculo do código *hash*[7] de quanto extraído (no arquivo UFDR, criado pelo software Cellebrite, este cálculo é automático) e armazenamento, em mídia apropriada, na Central de Custódia.
Neste procedimento o perito oficial abre o lacre aposto no aparelho no local e momento da apreensão, documentando e detalhando tal procedimento no laudo, e no fim dos trabalhos lacra novamente o aparelho, colocando o primeiro lacre (original) quebrado no mesmo invólucro e fazendo constar o número do novo lacre no laudo e/ou em outro relatório que irá compor a documentação da cadeia de custódia (Art. 3.7 da Portaria SENASP nº 82 e Art. 158-D do CPP).

5) Realização, sempre por parte de perito oficial, de cópias forenses integrais de tudo quanto extraído (arquivo UFDR com anexo o software gratuito de leitura, se tiver sido utilizado o sistema Cellebrite) para uso e análise das autoridades investigadoras, para juntada aos autos do processo (e consequente disponibilização ao Juízo, para que utilize tais provas para formação de seu livre convencimento motivado) e para disponibilização às Defesas.

[7] O cálculo do código hash é o principal sistema, reconhecido internacionalmente (inclusive na norma ABNT/ISO 27.037), para identificar de forma única um artefato digital (arquivo ou mídia), permitindo que se possa comprovar sua integridade, ou quebra de integridade, em qualquer momento futuro (a partir do momento do primeiro cálculo do hash).

pericias@ibracaf.com.br · 011-99271.2064 · www.parodi.in

No caso em foco, nenhum dos procedimentos acima foi realizado de acordo com as previsões legais, sendo que os procedimentos irregulares que foram adotados tiveram, entre outros, o efeito de quebrar a integridade e prejudicar totalmente a confiabilidade e higidez das evidências.

Ademais o comprovado acesso indevido ao aparelho antes do deferimento da quebra de sigilo por parte do Juízo, é uma questão adicional que faz com que a prova seja ilícita (além das outras ilicitudes).

A não adoção dos procedimentos de apreensão e custódia corretos, prejudica fatalmente a higidez e fiabilidade das provas, fazendo com que as mesmas devam ser consideradas inadmissíveis no âmbito de um processo penal democrático e de cunho acusatório.

Da mesma forma, encaminhar o material digital apreendido a seja quem for diferente da Central de Custódia e, sobretudo, permitir que tal material seja indevidamente manipulado (quem diga efetivamente modificado, como no caso em foco) por agentes diferentes dos peritos oficiais, configura uma insanável quebra da integridade da prova, que, de acordo com a jurisprudências prevalente das cortes superiores, resulta em sua inadmissibilidade para fins penais.

Pior ainda, por óbvio, se, como no caso em foco, tais outros agentes (diversos dos peritos oficiais) forem diretamente envolvidos nas investigações e, portanto, potencialmente interessados em tentar confirmar determinadas suas teses acusatórias, e, no momento das indevidas manipulações, inexistir a necessária autorização judicial para a quebra de sigilo de dados eletrônicos.

Cabe observar que, com a total ausência da cadeia de custódia (como no caso em foco), e pior, com a comprovada ocorrência de manipulações indevidas e da efetiva quebra da integridade do conteúdo do dispositivo alegadamente apreendido (arquivos modificados após a apreensão), passa a ser virtualmente impossível determinar o efetivo alcance das manipulações ocorridas e das modificações realizadas no conteúdo do aparelho.

Isso porque grande parte de tais adulterações pode ser realizada de forma indetectável, ou seja, sem deixar rastros.

Por esta razão, para garantir a autenticidade e integridade de tal tipo de material, é indispensável que todos os procedimentos que envolvam a custódia, o manuseio e, finalmente, a extração de dados do aparelho apreendido, sejam realizados por peritos oficiais, que, por sua função, tem independência funcional e não são envolvidos nas investigações nem comprometidos com a confirmação ou comprovação de determinadas teses.

Isso é, também, quanto expressamente previsto pelas vigentes normas aplicáveis (Arts. 158 a 159 do CPP, POP/2013 e portaria nº 82/2014 da SENAP, entre outras), que tem justamente o intuito de garantir a não contaminação e a preservação da integridade das provas.

Cabe relembrar que, em função da total ausência da cadeia de custódia, é até possível, em tese, que o aparelho que foi objeto da extração de dados espúria, não fosse aquele que foi efetivamente apreendido, podendo ter sido substituído por outro aparelho (independente da marca, modelo e cor, que não foram especificados no Auto de Apreensão), no qual tenha sido alterado o conteúdo, de forma a se coadunar com determinadas teses acusatórias.

Importante também salientar que, uma vez ausentes os corretos procedimentos de custódia e deixado o aparelho celular à mercê de seja quem for diferente dos peritos oficiais, mesmo a eventual posterior extração de arquivos por parte de perito oficial, porquanto eventualmente realizada de forma correta, não ostentaria mais a necessária garantia de autenticidade e higidez, pois é possível que durante o período sem adequada custódia tenham sido adulterados arquivos de todos os tipos (como, de fato, ocorreu), inclusive os bancos de dados de mensagens de aplicativos como o WhatsApp, se aproveitando da ausência ou quebra de custódia, como veremos mais à frente.

Por se tratar de prova digital, as eventuais alterações podem, inclusive, ter sido realizadas de forma virtualmente indetectável, fazendo com que, por consequência da ausência da cadeia de custódia seja inviável verificar a efetiva autenticidade de tais mensagens assim como de todo o conteúdo do aparelho celular em foco.

Isso significa que, por consequência da nítida ausência ou quebra da cadeia de custódia e, pior, da comprovada manipulação do aparelho por parte de quem esteve de posse deles após a alegada apreensão, é perfeitamente possível que supostas mensagens relatadas pelos investigadores como presentes no aparelho celular em foco, tenham sido, na realidade, criadas e/ou editadas, por parte de quem teve o mencionado indevido e livre acesso ao aparelho não custodiado, para se coadunarem com determinadas teses de acusação.

Da mesma forma, eventuais mensagens que não se coadunassem com as teses acusatórias pretendidas, podem ter sido excluídas, sempre de forma indetectável.

pericias@ibracaf.com.br · 011-99271.2064 · www.parodi.in

Infelizmente, como já mencionado, pela própria natureza das provas digitais, não é possível saber qual o efetivo e completo alcance das manipulações realizadas, se foram canceladas, criadas ou modificadas mensagens ou contatos (lembrando que o arquivo de banco de dados da agenda de contatos do aplicativo WhatsApp apresenta data de última modificação posterior à data a apreensão – Fig. 09 e 10) e quais, pois tais alterações realizadas em um banco de dados são, frequentemente, indetectáveis.

O mesmo vale em relação a praticamente qualquer outro arquivo alegadamente extraído do aparelho não devidamente custodiado desde o momento inicial de sua apreensão, de acordo com as normas aplicáveis.

Oportuno, ainda, salientar que, como adiantado, em muitos casos, é perfeitamente possível tanto editar mensagens de aplicativos como o WhatsApp, quanto criar do zero conversações falsas gravadas em smartphones.

O mesmo vale para imagens e outros tipos de arquivos, inclusive anexos às mensagens do WhatsApp, que podem ser criadas, modificadas, inseridas ou excluídas sem grandes dificuldades.

Para tanto é, obviamente, necessário ter livre acesso ao aparelho onde tais mensagens devem aparecer ou ser editadas (como, de fato, os investigadores tiveram, em relação ao aparelho em foco, inclusive tendo eles mesmos realizado a extração espúria dos dados).

De forma a exemplificar o quanto exposto acima (ou seja, como tais adulterações e edições podem ser facilmente realizadas, quando ausentes os corretos procedimentos de custódia), indicamos a leitura do artigo do Agente da Polícia Civil de SP (também expert em dispositivos móveis), Daniel Avilla, sobre "*Manipulação de mensagens e dados em dispositivos Android sem root*".

A matéria pode ser acessada através do seguinte link:
https://medium.com/@hubscherr2016/manipula%C3%A7%C3%A3o-de-mensagens-e-dados-em-dispositivos-android-sem-root-c6525b2e27d8

Cabe ainda observar que o sistema Cellebrite permite a adulteração do material extraído e incluído no arquivo UFDR a ser fornecido nos autos e às partes. Isso é possível em função de comprovadas vulnerabilidades do sistema Cellebrite, que foram, inclusive, objeto de artigos técnicos[8].

[8] https://www.conjur.com.br/2025-jul-18/vulnerabilidades-nos-arquivos-ufdr-da-cellebrite-impactos-e-riscos-da-cadeia-de-custodia/

Ou seja, por não terem sido, as extrações de dados, realizadas por perito oficial, não há como saber se o material fornecido como sendo aquele original presente no aparelho quando de sua apreensão, seja de fato autentico, integro e integral, ou tenha sido objeto de adulteração que pode ter ocorrido tanto no aparelho não devidamente custodiado, quanto após a extração espúria, diretamente no arquivo UFDR fornecido nos autos.

Os procedimentos de custódia, que visam garantir a autenticidade da fonte bem como a preservação da integridade das evidências e cuja indispensabilidade da adoção tem base constitucional, são previstos expressamente desde 2014 pela Portaria SENASP nº 82, são hoje detalhados pelos Arts. 158-A a 158-F do CPP (em vigor desde 23/01/2020), e têm fundamentação ainda mais forte no caso de provas digitais (como aquelas em exame). Isso porque, por sua natureza, a prova digital é, indiscutivelmente, muito frágil.

Na enorme maioria dos casos (e este é certamente o caso das provas em análise), provas deste tipo podem ser facilmente e rapidamente modificadas, inclusive, o que é mais grave, como já dito, de forma indetectável.

Como demonstrado acima, pode ser modificado (no sentido amplo, que inclui criação, alteração e cancelamento de dados) seu conteúdo, podem ser modificados metadados (blocos de informações estruturadas sobre características e história de um arquivo) e podem ser modificadas suas características (datas, autores, origem, identificação, nome, extensão etc.).

Diversas de tais modificações, em muitos casos, podem ocorrer em questão de minutos, o que faz com que seja crucial e de fundamental importância a adoção imediata e rigorosa dos corretos e completos procedimentos de custódia destas provas, desde o primeiro momento de sua aquisição e por parte dos agentes públicos legalmente competentes para tanto (no caso, de acordo com os mencionados artigos do CPP, tais agentes públicos são os peritos oficiais, lotados em Instituto de Criminalística, conforme definidos pela já mencionada Lei 12.030/2009), pois tais procedimentos e agentes são os únicos que podem permitir ter certeza quanto à manutenção da integridade, autenticidade e fiabilidade das provas digitais.

Isso também explica a especial necessidade de extremo rigor na correta gestão da cadeia de custódia das provas digitais, o que inclui sua identificação, o uso de lacres a partir do momento inicial da apreensão ou aquisição de outra forma, o registro documental dos procedimentos, a participação de perito oficial nos procedimentos de coleta, e, sobretudo, de remoção e custódia, desde o início e o imediato envio de quanto apreendido à competente Central de Custódia.

A não adoção dos procedimentos de custódia corretos, prejudica fatalmente a higidez e fiabilidade da prova, fazendo com que a mesma deva ser considerada inadmissível no âmbito de um processo penal.

Por vezes, no caso de provas digitais, se tem a ilusão que nada de relevante poderia ter acontecido no caso de uma custódia inadequada ou incorreta.

Na realidade sua fragilidade intrínseca faz com que as provas digitais sejam, provavelmente, um dos tipos de prova mais facilmente adulteráveis, sem deixar rastros.

Justamente a impossibilidade, por todas as partes e especialmente para a Defesa, de poder comprovar a ocorrência ou não de determinadas adulterações no caso de ausência da cadeia de custódia, em função de sua possível indetectabilidade, é o que gera o principal efetivo prejuízo para todas as partes do processo.

Para todos os efeitos práticos, a quebra ou ausência da cadeia de custódia (assim como outras irregularidades que resultem em dúvidas quanto à preservação da integridade, ou, pior, comprovem a efetiva quebra de integridade, como nos casos em foco) de uma prova digital, transforma a demonstração do efetivo prejuízo (ex vi Art. 563 do CPP), assim como qualquer outra possível demonstração relacionada à fiabilidade ou integridade da prova, em uma verdadeira prova diabólica.

Tudo isso faz com que todas as supostas provas digitais em foco, oriundas do mencionado aparelho celular alegadamente apreendido, não ostentem as mínimas características de fiabilidade, integridade e consistência epistêmica necessárias para que possam ser utilizadas para provar seja o que for, especialmente em âmbito penal.

Resumindo os principais pontos da análise dos documentos e do material digital fornecido, ao que foi possível averiguar e salvo eventuais omissões, temos que:

1) O aparelho celular sem descrição, identificado por um IMEI que não corresponde plenamente aquele indicado no arquivo UFDR da alegada extração de dados espúria, atribuído a Nelson Gomes Pereira Junior, apreendido em 10/05/2022 e sumariamente descrito no Auto de Apreensão nº 079776-1016/2022, não foi objeto dos devidos procedimentos de custódia pois:
   A) O aparelho não foi acondicionado de forma individualizados nem lacrado no momento da apreensão.

pericias@ibracaf.com.br · 011-99271.2064 · www.parodi.in

B) O aparelho foi removido do local da apreensão sem a prévia liberação do perito oficial responsável, em frontal afronta à explicita proibição prevista no Art. 158-C, § 2º do CPP.
C) O aparelho não foi imediatamente encaminhado à Central de Custódia, junto ao competente Instituto de Criminalística.

Em consequência de quanto acima, não é sequer possível saber se o aparelho que foi objeto da extração de dados seja, de fato, o mesmo alegadamente apreendido ou outro da mesma marca e cor (entre os mais comuns do mercado, diga-se de passagem), de origem desconhecida. Ademais, o Ato Administrativo da Apreensão, fica eivado de invalidade por ser ausente o requisito da Legalidade, em função do descumprimento da proibição prevista no Art. 158-C, §2º do CPP.

2) Ficou comprovado que, ao menos entre os dias 11/05/2022 e 15/05/2022 o aparelho foi manipulado extensivamente por quem esteve de posse dele, sem custódia, resultando na criação e/ou modificação de múltiplos arquivos de vários tipos, entre os quais arquivos de bancos de dados do aplicativo WhatsApp (mensagens e agenda de contatos).

3) Em 28/06/2022 foi realizada uma extração de dados espúria, pois realizada por assistentes técnicos da acusação (potencialmente comprometidos com a confirmação de suas teses acusatórias, sem isenção e sem garantias de manutenção da integridade – na realidade já previamente prejudicada). Tal extração de dados (e consequente quebra do sigilo de dados do aparelho), ademais, assim como as manipulações anteriores do aparelho, foi realizada sem prévia autorização judicial.

4) Somente em 14/10/2022 (meses após a realização da extração acima) foi deferida pelo Juízo competente a autorização de quebra de sigilo de dados eletrônicos, significado que as anteriores manipulações e acessos indevidos ao aparelho descritas no ponto anterior foram realizadas à revelia da Lei e das Garantias Constitucionais, resultando na contaminação da prova e fazendo com que a mesma passe a ser ilícita.

5) Em função de tudo quanto acima, e considerando as características das provas digitais, que podem ser facilmente modificadas (conforme demonstrado), inclusive de forma indetectável, não é possível excluir que muitos outros arquivos (além daqueles muitos, acima mencionados, que já ostentam data de modificação posterior à apreensão), armazenados no aparelho celular em foco, tenham sido excluídos, inseridos ou modificados após a apreensão, sem deixar rastros.

6) Considerando tudo quanto acima e especialmente a nítida ausência da cadeia de custódia do aparelho alegadamente apreendido, mais a comprovada quebra de integridade (ou seja, alteração) do conteúdo do dispositivo após a data da apreensão, mais a realização de procedimento de extração espúrio por parte da própria acusação, naturalmente interessada a confirmar suas teses acusatórias, inclusive em data anterior à autorização judicial para quebra do sigilo de dados eletrônicos, parece evidente que a consistência epistêmica, para fins probatórios, de tudo quanto alegado pela Acusação, com base no suposto conteúdo de tal dispositivo, seja certamente insuficiente para seu uso no âmbito de um processo penal de cunho acusatório, pautado nos princípios da presunção de inocência e da estrita legalidade.

   Adicionalmente, fica patente que em tais condições se encontra fatalmente prejudicado o exercício do contraditório e da ampla defesa, pois é impossível se exercer o contraditório e se defender em relação a supostas provas que, por exclusiva responsabilidade de quem as coletou, tratou e manuseou de forma indevida, foram eivadas por inúmeras irregularidades, acessos ilícitos, quebras de integridade e dúvidas quanto à sua origem, e autenticidade.

   O prejuízo, para o processo como um todo, é tão nítido e grave que nem sequer o próprio Juízo tem condição de saber se as provas que recebeu da Acusação, para dar lastro a suas alegações, são verdadeiras ou não.

   A prova da alegação incumbe a quem a fizer (Art. 156 do CPP), devendo, por óbvio, se tratar de prova válida, hígida, certamente autêntica e fiável.

   Quanto acima, também em consideração que “é do Estado o ônus de provar que atuou dentro dos contornos da legalidade”[9].

   Por outro lado a responsabilidade da preservação dos elementos de prova é do agente público que primeiro reconhecer tais elementos como de potencial interesse probatório[10], e que, por consequência disso, deveria ter tomado todas as providências de custódia explicitamente previstas nas normas aplicáveis (entre as quais os Arts. 158-A a 158-F do CPP e a própria Portaria SENASP nº 82/2014), o que não ocorreu.

[9] STJ, Sexta Turma, HC 915.025-SP, Rel. Min. Rogério Schietti Cruz, DJe 27/03/2025.
[10] Art. 158-A, § 2º do CPP e Art. 1.3 da Portaria SENASP nº 82 de 16/07/2014, publicada no D.O.U. de 18/07/2014: “O agente público que reconhecer um elemento como de potencial interesse para a produção da prova pericial fica responsável por sua preservação.”

▶ 4 - Conclusões

Encerrados os trabalhos, conforme acima descritos, esperamos ter explorado e trazido aos interessados às informações técnicas, fáticas e jurídicas necessárias, e colocamo-nos à inteira disposição para outros esclarecimentos julgados pertinentes.

Nada mais havendo a considerar, damos por encerrado o presente Laudo Técnico, constituído de 22 (vinte e duas) folhas numeradas de 1 a 22, todas de um só lado, todas redigidas pelo perito Lorenzo Parodi que subscreve e assina.

São Paulo, 19 de setembro de 2025

Lorenzo Parodi
Perito