O CÓDIGO "HASH" E OS EQUÍVOCOS DA DOUTRINA E DA JURISPRUDÊNCIA NA AVALIAÇÃO DA CADEIA DE CUSTÓDIA

O "fetiche" do código Hash, provas digitas e a cadeia de custódia

Fabrício Lamas Borges da Silva [1]
Douglas Fischer [2]

Introdução. O objetivo do presente texto, bastante pontual e objetivo de forma proposital, é demonstrar ao leitor dois grandes equívocos que estão ocorrendo no que se refere à cadeia de custódia da prova digital e também quanto ao denominado "Código Hash". Mostraremos que são muitas as decisões que, reconhecendo a quebra da cadeia de custódia, entendem que não há, automaticamente, a nulidade das provas produzidas, embora outras, paradoxal e, em nossa concepção, contraditoriamente, tratem do tema pelo prisma da confiabilidade probatória. Demonstraremos que é equivocado tratar o tema da cadeia de custódia na seara das nulidades e/ou invalidades, bem assim que há uma grande confusão teórica e técnica acerca do "Código Hash", muito "falado" e pouco compreendido, e, em algumas circunstâncias, menções completamente equivocadas acerca do que significa referido código, de sua utilidade e dos significados de sua ausência ou não verificação.

O que é a cadeia de custódia ?

Inicialmente é importante consignar que a *regulamentação* da cadeia de custódia no CPP com a Lei nº 13.964/2019 não trouxe, tecnicamente, nenhuma *inovação* quanto à necessidade – sempre existente até então – de se garantir a custódia da prova. Houve tão somente a inserção desse protocolo (que não é procedimento processual de produção de prova) no âmbito da legislação processual penal. E a finalidade do *protocolo – dividido em dez etapas* - sempre foi a preocupação com a fidedignidade e não alteração do estado dos vestígios do crime, desde a coleta até a ulterior apreciação pelo Poder Judiciário. Não foi o fato de essas "etapas" terem sido inseridas no Código de Processo Penal que as "transformaram", tecnicamente, em um "procedimento processual penal".

1 Promotor de Justiça do Estado de Goiás. Coordenador do CyberGAECO do MPGO, Lattes.cnpq.br/1465839215500148

2 Procurador Regional da República na 4ª Região, Professor de Direito Processual Penal, Mestre em Instituições de Direito e do Estado pela PUCRS, LATTES.cnpq.br/5240252425788419

Toda prova que embasa um processo penal tem a finalidade de buscar o chamado "acertamento jurídico dos fatos", observando-se todos os princípios norteadores do devido processo *(que, deixamos também aqui expresso, não está destinado a proteger apenas os interesses dos investigados ou processados, mas também das vítimas e preservar o interesse da coletividade, consoante já reiteradamente reconhecido pela Corte IDH)*. Exatamente nesse sentido é que colacionamos excerto de decisão do STJ em que, embora rara e tratando de arguição de *nulidade* de provas por suposta quebra da cadeia de custódia, reconheceu que "*a busca do acertamento fático é elemento do justo processo penal".* Assim, é "*fundamental que haja, com o respeito aos direitos fundamentais do réu, de eventual vítima e da sociedade, a correspondência, ao menos aproximada, entre os fatos, tal como ocorreram, e aqueles descritos nos autos. E o campo para dirimir dúvidas é o juízo da causa, sob o contraditório judicial".(RHC nº 104.176/RS, STJ, 6ª Turma, unânime, Rel. Min. Rogério Schietti Cruz, julgado em 4.5.2021, publicado no DJ em 14.5.2021).*

É preciso sedimentar de plano que a cadeia de custódia não se confunde com atividade de produção de prova em si. Esse *protocolo* (que não é *procedimento processual* penal, repita-se) tem a finalidade única de garantir a *confiabialidade* da prova licitamente coletada.

Decorrência lógica do que foi dito, ainda reproduzindo aquele entendimento, *não se deve falar em invalidade em eventual caso de quebra da cadeia de custódia, mas de ausência de segurança acerca do seu conteúdo*[1].

Além de não ser uma *novidade quanto a sua exigência*[2], vamos falar de forma repetitiva que o sistema de aferição da cadeia de custódia *não é* um *meio de produção probatória,* mas um *protocolo* que procura garantir a fidedignidade da prova *já produzida/obtida licitamente*, de que a prova possui a origem descrita (que é autêntica) e que não sofreu alterações significativas (permanecendo íntegra).

Significa que a cadeia de custódia pressupõe logicamente que a prova produzida seja *lícita,* pois, do contrário, tecnicamente não mais há necessidade de discussões, na medida em que essa prova não poderá ser utilizada no processo penal, por expressas vedações convencional, constitucional e legal.

Jamais defenderemos – também aqui - que sejam adotados procedimentos contrários ao que previsto em regulamentos administrativos (como era o tema da cadeia

de custódia até então), noutras normas ou até mesmo no Código de Processo Penal (embora *não seja* em si algo relacionado *à produção probatória*), mas é preciso ver que eventual não observância do que previsto nos estritos detalhamentos legais (das "etapas") não conduzem a discussão ao sistema de *invalidades/nulidades*, mas na *segurança suficiente de que aquele vestígio* coletado pode servir para valoração ou não pelo julgador, especialmente para fins de condenação (mas ele servirá também muitas vezes para a absolvição, não pelo prisma de *prova ilícita*, que pode ser utilizada em prol da defesa*, mas no campo da confiabilidade*/segurança).

Importante sempre reportar das precisas considerações de Antônio Graciano Suxberger em seu texto *"Cadeia de Custódia como meio de identificação da prova: a interseção entre a probática e a epistemologia probatória"* [4]. E já alertamos que se mostra equivocado *mesclar, confundir* ou até mesmo desvirtuar a discussão acerca da cadeia de custódia para o campo das *nulidades/invalidades* probatórias.

Partamos da premissa de que cadeia de custódia nunca foi um *meio de produção probatória,* mas de um "protocolo investigatório", o que, como adverte Suxberger, tem *"conduzido ao enfrentamento do tema como se tema de nulidade processual fosse ou, o que é pior, como se fosse tema de ilicitude (e, portanto, de inadmissibilidade) probatória"* (p. 25).

O que muitos não atentam é que a razão de ser da cadeia de custódia consiste justamente em assegurar os exames de mesmidade e integridade do vestígio. A cadeia de custódia, como protocolo de atuação dos órgãos de persecução do Estado, permite a extensão do caminho de racionalidade das decisões judiciais ao momento da investigação preliminar que resultou na identificação e coleta do vestígio.

Como se vê da legislação, não há previsão dos efeitos do seu eventual descumprimento, muito menos não há um detalhamento acerca da valoração das provas. É que, diferentemente *de onde importada*, a cadeia de custódia ("chain of custody") deve ser analisada *previamente* pelo juiz porque a *valoração* (dessas provas) será feita normalmente pelos *jurados* (sem necessidade de *fundamentação*).

A cadeia de custódia *não trata de uma formalidade de ato processual*, motivo pelo qual eventual quebra (jamais defendida por nós, que fique novamente bem registrado inclusive nesse texto) induzirá que o elemento de prova é *imprestável* ou *ilícito,* como se queira. Ela *pode deixar de ser confiável* para embasar a decisão judicial,

mas jamais poderá ser “excluída” da apreciação do juiz, que deverá a analisar à luz especialmente do disposto no art. 155 do CPP.

Com a vênia de posicionamentos em contrário, a cadeia de custódia não é um *pressuposto* e muito menos um *requisito* de *validade* da prova (já produzida anteriormente de forma *lícita*). Exatamente por isso é que eventual não observância dos passos do *protocolo* da cadeia de custódia não resulta tecnicamente em *nulidade da prova* (salvo se tiver adulteração que comprometa a própria essência do vestígio em si).

Eis a razão pela qual concordamos novamente com Suxberger: *O risco de equívoco dessa “passagem” encontra-se na assunção equivocada de que a inobservância da regra probatória implica inobservância de regra dirigida à validade de ato processual. Não é o caso. Trata-se de apreciar a creditibilidade e prestabilidade para convencimento da prova técnica (p. 35).*

Definitivamente não concordamos (e, *venia concessa,* consideramos *equivocados)* posicionamentos que defendem – e literalmente misturam, *data venia* – os conceitos de fiabilidade, validade e ilicitude de provas.

Dentro de uma concepção racionalista do sistema probatório, deve-se atentar que, se no curso da *preservação* dessa prova (“cadeia de custódia”) houver alguma falha, esse *vestígio/prova* não é *transmudado* para o *campo da ilicitude*, mas deverá ser analisado (e *não excluído da* apreciação), mediante a devida fundamentação, se ela serve para o fim probatório e qual o limite de convencimento do julgador.

Se houver dúvida acerca da “suficiência” dessas provas no bojo de um processo penal, a solução é bem clara: absolvição. Mas se ela *tem* fiabilidade, ela não apenas poderá como deverá ser *valorada* pelo julgador, preferencialmente em conjunto com os demais elementos produzidos. Exatamente por isso, encontramos na jurisprudência do STJ (com dissensos inexplicáveis para nós) que "*se é certo que, por um lado, o legislador trouxe, nos arts. 158-A a 158-F do CPP, determinações extremamente detalhadas de como se deve preservar a cadeia de custódia da prova, também é certo que, por outro, quedou-se silente em relação aos critérios objetivos para definir quando ocorre a quebra da cadeia de custódia e quais as consequências jurídicas, para o processo penal, dessa quebra ou do descumprimento de um desses dispositivos legais"*. A conclusão foi no sentido de que se mostra "*mais adequada a posição que sustenta que as irregularidades constantes da cadeia de custódia devem*

ser sopesadas pelo magistrado com todos os elementos produzidos na instrução, a fim de aferir se a prova é confiável. Assim, à míngua de outras provas capazes de dar sustentação à acusação, deve a pretensão ser julgada improcedente, por insuficiência probatória, e o réu ser absolvido. [...] (*Habeas Corpus nº 653.515/RJ, STJ, 6ª Turma, por maioria, Rel. Min. Rogerio Schietti Cruz, julgado em 23.11.2021, publicado no DJ em 1º.2.2022).*

Não se olvide jamais que a atividade probatória tem a finalidade de busca do *acertamento dos fatos* do processo, pois *justo processo* compreende a apuração da verdade (exatamente como propugna *Ferrajoli)*.

A "mescla" de conceitos de fiabilidade/mesmidade com invalidade/nulidade das provas quando há quebra da cadeia de custódia.

Atualmente muitas posições jurisprudenciais são "sedimentadas" a partir de *citação* especialmente de ementas de julgados anteriores. O grande "problema", dizemos nós, é quando as premissas desses julgados se apresentam de forma equivocada. A consequência é que a repetição dessas "inverdades" (no sentido de falta de tecnicismo para apuração do que efetivamente seja a *cadeia de custódia*) acaba gerando uma repetição em cascata de premissas que não são corretas. Por consequência, as conclusões igualmente não podem ser defensáveis, especialmente porque mesclam e confundem os temas.

Não reportaremos aqui os julgados, basta pesquisá-los. É incrível a confusão conceitual que é realizada. São reiterados julgamentos em que se vê a utilização dos argumentos da *confiabilidade da prova* e da *nulidade* dela como se fossem interligadas.

Se uma prova é *ilícita* (inválida), sequer caberia ao julgador fazer a análise da sua *confiabilidade*. *Uma exclui a outra.*

A prova ilícita não pode ser usada no processo. A prova lícita, mesmo com a quebra da cadeia de custódia, tem que ser analisada para saber se confere *credibilidade* para o julgamento. Ou seja, ela tem que ser avaliada pelo julgador e não eventualmente *excluída*.

Exatamente por isso é que, tratando especificamente de possível quebra na cadeia de custódia de *provas digitais* extraídas de aparelho celular (se é hipótese de comprometimento da confiabilidade e enseja nulidades ou não), encontramos em decisões do STJ o expresso reconhecimento de que "a jurisprudência consolidada do

STJ estabelece que irregularidades na cadeia de custódia devem ser sopesadas pelo magistrado com todos os elementos produzidos na instrução, para aferir se a prova é confiável" *(Agravo Regimental no Habeas Corpus n° 1.007.891-ES, STJ, 5ª Turma, Rel. Min. Messod Azulay Neto, julgado em 13.11.2025, publicado no DJ em 14.11.2025)*.

O que pode causar perplexidade – diferentemente da parte final do caso acima - é que, em vários julgados, colhe-se a clara distinção entre *nulidade da prova* e *fiabilidade da prova*, sem que se veja nesses casos uma justificação ou *distinguish* para o tratamento fora dos parâmetros aos quais acima destacado.

Mencionamos aqui também decisão *monocrática* de 27 de março de 2026, exarada pelo Ministro Cristiano Zanin no bojo do Habeas Corpus nº 242.921-DF. Nesse caso, sua Excelência concedeu efeito extensivo (art. 580 do CPP) para *anular* condenação criminal em relação ao paciente do feito, pois já havia decisão colegiada anterior da 2ª Turma do STF (transitada em julgado) anulando a condenação de outros envolvidos no mesmo feito. Nesse caso anterior, o STF reconheceu que "*da detida análise das razões de decidir adotadas pelas instâncias de origem, conclui-se facilmente o rompimento da cadeia de custódia e a ausência do exame pericial em material extraído de equipamento eletrônico, o qual ancorou substancialmente a prolação do édito condenatório, em manifesta violação do disposto nos arts. 158 e 158-A, do Código de Processo Penal"*.

Na verdade, foram licitamente extraídas (ordem judicial) informações de computadores mediante cópias em "pendrives". Por isso, seguindo no raciocínio do julgamento colegiado,

> à míngua da realização de perícia no computador da Secretaria Municipal de Desenvolvimento Humano e Social de Campos dos Goytacazes/RJ, de onde foram extraídos os dados impugnados, constata-se facilmente que não é possível assegurar, com segurança e de forma indene de dúvida, a autenticidade dos elementos informativos coligidos por meio de um pendrive. Evidentemente também não é possível garantir a idoneidade da fonte dos dados ou a cadeia de custódia, uma vez que, conforme explicitado pelas instituições judiciais de origem, não houve a preservação do ambiente original para perícia, impedindo a realização de contraprova, o que malfere as citadas regras sobre a cadeia de custódia bem como os princípios do contraditório (art. 5º, LV, CF), do devido processo legal (art. 5º LVI, CF) e, por consequência, da inadmissibilidade das provas ilícitas (art. 5º, LIV).

Aqui começa o "problema", em nossa compreensão. Não se discute aqui se as outras provas seriam "suficientes ou não" para manter o édito condenatório, mas não se assevera correto, juridicamente, dizer que essa providência de extração de dados – tal como realizada - "transformaria" as provas coletadas em "provas ilícitas". O acesso às provas foi absolutamente *lícito*, pois precedido de devida e autorizada *busca e apreensão.*

Veja-se que, na sequência do julgado, encontra-se a seguinte fundamentação (o que demonstra haver "clara confusão" conceitual): "*Rememoro, a propósito, que a cadeia de custódia da prova, prevista nos arts. 158-A a 158-F do Código de Processo Penal com o advento do 'Pacote Anticrime' (Lei 13.964/2019), disciplinou o conjunto de procedimentos a serem observados durante a coleta das provas em processo penal, visando à preservação da integridade da prova colhida, com a finalidade de assegurar a verificação de sua autenticidade pelas partes e pelo Juízo".* Ou seja, fica claro aqui que a premissa é (correta) de que a cadeia de custódia visa garantir a fidedignidade da prova.

Aqui um "salto hermenêutico" novamente. Como não houve *perícia* nos computadores, para verificar se as provas insertas nos pendrives eram as mesmas dos dispositivos originários (e não há *nenhuma prova de que não sejam*, senão apenas as alegações unilaterais de que o procedimento *pericial não foi realizado*), a conclusão do silogismo do voto-condutor foi no sentido de que "*parte do material que fundamenta a condenação do recorrente está tisnado de irregularidade. Por tal motivo a sanção processual cabível é a decretação de nulidade do édito condenatório ante o reconhecimento da ilicitude e, na hipótese da impossibilidade de perícia da fonte primária (computador), a ser enfrentada pelo juízo de origem, o desentranhamento da prova documental coligida a partir da busca e apreensão, nos termos do art. 157 do CPP*".

Equívoco dos mais graves também aqui, *data venia*.

Há clara mescla e confusões dos institutos e dos conceitos.

Se houvesse efetivamente a demonstração de *diferença de provas* (inserta nos computadores daquelas dos pendrives), o que jamais ocorreu (senão apenas a *alegação da ausência de perícia*), a conclusão deveria ser no sentido de que as provas utilizadas

no processo eram *não seguras* para o édito condenatório, mas jamais – jamais ! - reconhecer que a prova originária seria *ilícita,* gerando, por arrastamento (*fruits of the poisonous tree)*, a *invalidade* das provas coletadas a seguir. Não poderia a Corte Suprema incorrer em tamanho equívoco de raciocínio jurídico, senão e exclusivamente por conta de confundir – e talvez não bem compreender, ainda – o que significa a cadeia de custódia das provas.

Evidentemente que se houvesse uma demonstração (ônus de quem alega, art. 156, CPP) de que as provas utilizadas foram eventualmente *adulteradas,* aí sim se poderia cogitar em imprestabilidade das provas, se esse vício acabasse por acertar em cheio na própria essência do conteúdo probatório utilizado para o édito condenatório.

No mesmo vício de premissas também incorreu o STJ ao julgar o Agravo Regimental no Habeas Corpus n° 901.602 - PB (5ª Turma, por maioria, Rel. Min. Reynaldo Soares Da Fonseca, Redatora do acórdão Min. Daniela Teixeira, vencidos Reynaldo Soares da Fonseca e Ribeiro Dantas, julgado em 12.2.2025, publicado no DJ em 11.3.2025). Nesse caso, o réu tinha sido pronunciado pela suposta prática dos crimes de homicídio doloso, na forma simples, e lesão corporal, em razão de fato ocorrido no ano de 2013. A acusação baseou-se em vídeos supostamente extraídos de câmeras de segurança, cuja autenticidade e fidedignidade foram questionadas pela defesa. Discutia-se no feito se a ausência de documentação adequada sobre a cadeia de custódia das provas (filmagens) compromete sua integridade e fidedignidade.

A Corte Superior disse inicialmente que a "*cadeia de custódia visa garantir que os vestígios de uma infração penal correspondam exatamente àqueles arrecadados pela polícia, examinados e apresentados em juízo, assegurando sua integridade". Mas, a seguir, assentou algo que realmente revela total confusão conceitual, na medida em que disse que "a quebra da cadeia de custódia torna inadmissíveis as provas extraídas, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP"*. Desse modo, também nesse caso, concedeu-se a ordem para anular o processo desde a decisão de pronúncia e declarando a nulidade das filmagens utilizadas nos autos, pela quebra da cadeia de custódia.

Noutro caso, também envolvendo "provas digitais", o STJ discutia se teria havido *"violação da cadeia de custódia das provas digitais extraídas do celular apreendido, comprometendo sua integridade e confiabilidade". Reconheceu-se que a autoridade policial manuseou o celular do corréu, confrontando-o a respeito do seu*

conteúdo, extraindo prints de conversas por aplicativos e elaborando relatório antes do encaminhamento ao Instituto de Criminalística, comprometendo a fidedignidade da prova". Aí a conclusão do aresto: *"a quebra da cadeia de custódia foi constatada, pois não foram adotados procedimentos que assegurassem a idoneidade e a integridade dos dados extraídos"*. Como o "*ônus de comprovar a integridade e confiabilidade das provas cabe ao Estado, não sendo possível presumir a veracidade das alegações estatais sem a devida documentação da cadeia de custódia*". Desse modo, a conclusão da tese decisória foi no sentido de que a "*quebra da cadeia de custódia de provas digitais compromete sua fidedignidade e integridade. 2. O Estado tem o ônus de comprovar a integridade e confiabilidade das provas apresentadas. 3. A ausência de documentação da cadeia de custódia torna a prova inadmissível no processo penal" (Agravo Regimental no HC nº 943.895-PR, STJ, 5ª Turma, Rel. Min. Joel Ilan Paciornik, julgado em 4.9.2025, publicado no DJ em 5.9.2025).*

A par dessas conclusões acima (equivocadas, respeitosamente), destacamos outra decisão, do mesmo órgão colegiado do STJ, em data relativamente próxima, também tomado por unanimidade, porém com conclusões de mérito em sentido contrário *(Agravo Regimental no Recurso Especial n° 2.118.472-TO, STJ, 5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 26.2.2025, publicado no DJ em 6.3.2025).* Nesse feito, a questão em discussão era saber "s*e a condenação pode ser mantida com base em provas testemunhais e prints oriundos de conversas de WhatsApp, sem perícia"*. Considerou-se que a *"condenação foi mantida com base em provas testemunhais coesas e harmônicas, além de prints de conversas de WhatsApp, que, embora não periciados, não apresentaram indícios de adulteração*". Por essa razão, corretamente dizemos nós, foi denegada a ordem, na medida em que a prova digital (*prints* de *whatsapp, devidamente valoradas pelo julgador – como deve ser)* estavam em harmonia com os demais elementos probatórios, não se falando em *nulidade processual.*

Embora se pudesse analisar vários outros feitos (o que se fez foi apenas exemplificativamente), e novamente com o devido respeito, por todas as razões destacadas anteriormente, não nos parece correto abrir discussão sobre *nulidade/invalidade* das provas se, como premissa, a discussão está centrada (ou pelo menos admitida) na *fiabilidade* ou *credibilidade* das provas.

Repetimos: para nós, os argumentos são excludentes entre si. Não se pode falar em credibilidade e admitir que eventualmente não há nulidade porque ausente prejuízo

(de fato, sempre escrevemos sobre o tema e explicamos detalhadamente as razões jurídicas pelas quais está correto fazer, de regra, a ponderação de prejuízo – art. 563, CPP – independente de que *tipo de nulidade* se diga, absoluta ou relativa[5].

A compreensão do "código hash" e as imprecisões e equívocos técnicos difundidos na doutrina e na jurisprudência.

Aqui reside um dos pontos críticos do presente texto: há muitas doutrinas e decisões que se reportam ao "Código Hash" sem mesmo compreender na essência o que ele significa. Pior são posicionamentos que invocam teorias de exclusão probatória quando a legislação pátria expressamente adverte acerca das especificidades do mencionado meio de aferição.

Desde já destacamos que haverá muitas remissões a texto muito mais completo e detalhado do coautor Fabrício Lamas (vide *A garantia da integridade da Prova digital com Código Hash: uma análise crítica),* de modo que haverá uma identidade parcial de fundamentos (evidentemente que não explorando todo o complexo lá abordado).

Provas digitais relacionam-se à forma dos seus "registros", que se dá em forma de "bits", que são a menor unidade de armazenamento da computação, onde tudo pode ser representado por "0" ou "1". Portanto, o que temos e vemos num documento digital são combinações de muitos bits nesses formatos.

Um conceito importante ao começar a tratar desse tipo de "prova" é que elas são consideradas "voláteis", no sentido de que elas podem ter seu conteúdo total ou parcialmente perdido ou alterado ao longo do tempo, bem assim podem ser adulteradas. Mas essa volatilidade não existe apenas nessas provas. A mais tradicional prova do processo penal, a testemunhal, é uma das mais voláteis exatamente pela sua própria natureza. Exatamente por isso é que é bastante comum que testemunhas não se lembrem de todos detalhes do que presenciaram ao prestar o depoimento. Mas nem por isso se considera que as provas testemunhais (talvez as mais "suscetíveis a adulteração") são imprestáveis ou devam ser excluídas por conta da ausência de detalhes não lembrados. Elas precisam ser analisadas como toda e qualquer prova, desde que lícita. Trata-se da credibilidade da prova, não da *validade*.

Vemos em doutrina posicionamentos como de Gustavo Badaró *(A Cadeia de Custódia da Prova Digital, de 2021)*, em que afirma que a prova digital é dotada de volatilidade e fragilidade, sendo facilmente passível de ser "contaminada". Desse modo,

recomenda a adoção do uso do algoritmo “hash” nas provas digitais, bem assim de técnicas como a ABNT-NBR ISO/IEC 27037:2013, como condições para serem “aceitas” as provas digitais num processo criminal. Considera que esses padrões metodológicos seriam os mais adequados para provar a veracidade dos fatos, concluindo que se as provas porventura não seguirem o que considera de “melhores práticas” não poderão ser admitidas, adotando-se, quanto a elas, o mesmo rigor das provas ilícitas ou ilegítimas. Tal raciocínio é facilmente verificável em vários julgados, inclusive do STJ, que estão adotando sem maiores critérios, fiando-se exclusivamente na ponderação do referido autor.

O que verificamos é que se está gerando algo que podemos denominar de “fetiche do hash”, que pode ser assim resumido: *“se tem código hash, a prova é válida e poderá ser trazida nos autos; mas se não tem código hash, a prova deve ser descartada, independentemente se ela possa ser ou não corroborada por outros meios probatórios existentes. Não se discute valor probatório, mas aceitação ou não da prova”* (Fabrício Lamas Borges da Silva, 2026).

É preciso fazer alguns alertas importantes.

Primeiro, que a principal norma internacional sobre provas digitais, a NBR ABNT/ISO/IEC 27037:2013, recomenda expressamente que ela *não deve susbtituir* exigências legais jurisdicionais. É dizer, essa norma não trata de metodologia para procedimentos judiciais. A própria norma traz expressa recomendação de que isso não seja feito. Portanto, doutrinas que recomendam o uso de normas técnicas desse jaez estão contrariando uma recomendação da própria norma técnica nacional e internacional sobre o assunto, incorrendo em um paradoxo, pois ***seguir tais normas como substituto de exigência legal é uma desobediência expressa ao que essas normas recomendam.***

Com todas as letras, precisamos reiterar que, ao contrário do que sustentado por Badaró, *“a norma técnica NBR ABNT/ISO/TEC 27037:2013 não recomenda a exclusão nem mesmo de provas que tenham sido espoliadas (nome técnico dado à evidência digital alterada) e reconhece apenas a diminuição de seu valor probatório. Nesse sentido, ao conceituar a espoliação da evidência (item 3.19), a norma técnica afirma expressamente que a consequência automática é que isso diminui o valor probatório – e não que não dispõe que ela deve ser descartada”* (Fabrício Lamas Borges da Silva, 2026).

Em outras palavras, a norma *NBR ABNT/ISO/TEC 27037:2013* traz de fato boas práticas a serem seguidas (e que recomendamos, por óbvio), mas não dispõe que uma prova coletada sem algum de seus pressupostos deva ser descartada ou equiparada a uma prova ilícita, tratando tais provas como provas *válidas* mas com *menor valor probatório* – as quais por óbvio deverão ser analisadas dentro do conjunto de provas existentes em um processo.

Segundo. É equivocado considerar que se o código *hash* estiver alterado o documento que os bits representam foram adulterados, de modo que deve ser "descartado".

O código *hash* é o nome dado a um código alfanumérico de tamanho fixo, a partir de cálculos matemáticos e que pode ser gerado a partir de qualquer documento digital. Na verdade, o conceito *de hash* surgiu há muito tempo, quando não se discutia ainda o armazenamento de provas digitais. O *hash* de criptografia atual tem a capacidade de detectar a existência de qualquer alteração mínima num arquivo, mas não possui capacidade de indicar o tamanho, o alcance e o que significam essas alterações.

O *hash* determina a integridade de um determinado documento. Alterando-se um bit, altera-se completamente o *hash*, gerando ainda o chamado *efeito avalanche*, que repercute em todo o "código" (que é gerado a partir de um cálculo matemático, como dito).

Fabrício adverte ainda que *"a alteração de um único bit, capaz de gerar um hash completamente diferente, pode ser: a) invisível a olho nu; b) irrelevante para a computação; c) decorrente de fatores alheios a qualquer ação ou omissão humana. Nestes três casos, apesar da alteração do código hash, não haveria alteração ontológica que justificasse a exclusão ou não da anállise de uma prova digital"*.

Em outras palavras, dois arquivos com similaridade de 99,99999...% de *bits* (sendo que o segundo pode ter sido alterado por circunstâncias incontrolável, como verá), com documentos que tenham essencialmente o mesmo conteúdo, terão um código *hash* completamente diferente, por conta do efeito avalanche.

Considerar que uma prova – com um *hash* diferente por conta de poucos bits (e do efeito avalanche) – deva ser excluída ou equiparada a prova ilícita (como um depoimento colhido sob tortura, por exemplo) é, com o devido respeito, tão "coerente" como seria descartar completamente um depoimento testemunhal porque alguém não se

lembra de algum detalhe do dia dos fatos (como uma cor de uma camiseta de alguém que estava no local) ou descartar uma prova documental porque um milímetro de um canto da folha foi danificado. Se esse raciocínio tão exigente – aplicado às provas digitais - fosse estendido para as demais provas, talvez pouquíssimas provas resistiriam e poucos processos chegariam a uma conclusão.

Até porque o que não é dito é que as alterações de bits também podem ocorrer automaticamente, sem qualquer intervenção humana. É que isso é um fenômeno bastante comum conhecido como *corrupção silecionada de dados (SDC – silent data corruption),* erros silenciosos de dados ou "apodrecimento" de bits, tudo decorrente de fatores físicos, ambientais e quânticos que comprometem a integridade dos *bits* armazenados em sistemas. Bastante comum é a influência da temperatura e umidade que, alterando um bit, geram a modificação total dos hashes (pelo efeito avalanche). Porém os documentos, em si são, na essência, idênticos. Ontologicamente idênticos, porém com códigos hash diversos.

De fato, seguindo ainda o que já dito noutro espaço, pode ocorrer, exemplificativamente, que *"um HD contendo cópia de material criminoso de abuso sexual infantil, enquanto prova digital tenha algum bit alterado por conta de fatores involuntários e mude completamente seu hash (por conta do efeito avalanche), sem que nem mesmo esse HD tenha sido deslacrado, que algum arquivo tenha sido aberto ou que se gere alguma imagem com diferença visível a olho nu. E, por conta da unidirecionalidade, não será possível nem sequer entender o motivo da alteração. O arquivo – com alteração mínima – continuará ontololgiamente o mesmo, com hash diferente. Continuará comprovando o crime apresentando o mesmo conteúdo visual"* (Da Silva, 2026).

E quando se leva este raciocínio para *smartphones* (local onde estão grande parte das provas processuais digitais) a situação é ainda mais complexa. Isso porque tais aparelhos, por possuírem, além da memória de armazenamento tradicional, espaços de memória volátil – "memória RAM" - dentro dele, qualquer alteração automática decorrente da própria natureza do aparelho (sem qualquer ação ou omissão humana) alteram completamente o código *hash* de sua extração (pelo efeito avalanche), de forma absolutamente incontrolável, sendo praticamente impossível repetir o *hash* de duas extrações de um mesmo aparelho celular (mesmo ele tendo o mesmo conteúdo).

A irrepetibilidade de código hash em aparelhos com memória volátil é esclarecida pela própria NBR ABNT/ISO/IEC 27037: 2013 (ABNT, 2013), que dispõe que "*é recomendável que o DEFR (nome dado pela norma a quem faz aquisição de prova) esteja atento a possíveis* ***circunstâncias em que não será possível repetir o teste****, por exemplo, quando um disco rígido original foi copiado e voltou a ser utilizado* ***ou quando um item envolve memória volátil****. Nestes casos, convém que o DEFR assegure que o processo de aquisição é confiável"* – destacou-se.

Essa irrepetibilidade já foi comprovada cientificamente pela literatura internacional, com testes (Cuomo, D'Agostino e Ianulardo, 2022) e também foi já detalhada em artigo em português escrito pelo coautor Fabrício em conjunto com Emerson Wendt (Da Silva e Wendt, 2024).

Ao se tratar uma prova pela não repetição ou ausência de código *hash* como nula – equiparando a uma prova obtida sob tortura, por exemplo – tem menos sentido ainda quando analisamos essas exigências em extrações vindas dos aparelhos telefônicos modernos.

Atente-se que a não repetição de *hash* não significa sequer que o conteúdo encontrado em algum lugar foi alterado – já que a alteração pode ser de um único *bit* e por circunstâncias incontroláveis (físicos, ambientais e até mesmo quânticos) ou mera existência de memória volátil. Portanto, defender a "invalidação" de um documento digital porque o código *hash* não é mais o mesmo não coerência lógica científica. A alteração do código pode decorrer de muitos fatores, sem que isso signifique "adulteração" ou perda da fidedignidade da prova.

Conclusões.

O sistema de aferição da cadeia de custódia *não é* um *meio de produção probatória,* mas um *protocolo* que procura garantir a fidedignidade da prova já produzida *licitamente*.

É equivocado *mesclar, confundir* ou até mesmo desvirtuar a discussão acerca da cadeia de custódia para o campo das *nulidades/invalidades* probatórias. A inserção do *protocolo* de cadeia de custódia no âmbito do Código de Processo Penal não transformou num *requisito de validade* da prova. Assim, a cadeia de custódia *não trata de uma formalidade de ato processual*.

Ao tratarmos da *cadeia de* custódia, não um procedimento *processual* de *produção probatória*, mas um *protocolo* para a *manutenção dos vestígios coletados licitamente (para garantir a mesmidade e integridade),* para nós não se apresenta como mais correto epistemicamente incursionar na discussão de *invalidade/validade* das provas quando o debate está atrelado ao *protocolo* das provas *lícitas* que poderão ter afetar a *credibildade* ou *fiabilidade* no momento da avaliação pelo julgador.

A eventual alteração do código *hash* de provas digitais não significa automaticamente que a prova foi "adulterada" ou "modificada" ou mesmo que não foram tomados cuidados adequados. Há vários fatores que podem conduzir, mesmo sem a ação humana, para a *modificação* do código hash, sendo isso comprovado cientificamente.

A quebra da cadeia de custódia no sistema jurídico brasileiro, mesmo na seara das provas digitais, não pode levar à *exclusão* da prova, muito menos à declaração de sua *ilicitude*, pois, como insistentemente dito, não é disso que trata o *protocolo* legal inserto no Código de Processo Penal que, agora, detalha a *cadeia de custódia,* desde a colheita até o descarte das dos *elementos probatórios* (*evidence*) lícitos.

Criar exigências que contrariam a lógica e a ciência, bem como consequências absurdas e exageradas ao descumprimento de formalidades de normas técnicas (que nem essas próprias normas técnicas recomendam), equiparando a mera ausência de um mecanismo de confiabilidade de prova, como *hash,* a uma prova ilícita, não gerará um processo penal justo, mas será fator de aumento de injustiças no processo penal brasileiro com resultados nefastos.

Referências bigliográficas.

Brandalise, Rodrigo; Fischer, Douglas. A Cadeia de Custódia e a prova digital: uma análise a partir da decisão do Superior Tribunal de Justiça no AgRg no Aresp 2.309.888-MG

Da Silva, Fabrício Lamas Borges. A garantia da integridade da prova digital com código hash: uma análise crítica. In Tratado de Investigação Digital. Vol 1: Prova, Técnicas e Ferramentas. Porto Alegre: WB Educação, 2026.

Oliveira, Rafael Serra. Cadeia de custódia no processo penal. São Paulo: Thomson Reuters, 2025

Pacelli, Eugênio; Fischer, Douglas. Comentários ao Código de Processo Penal e sua Jurisprudência, Juspodivm: Salvador, 2026, 18 ed.

Pereira, Frederico Valdez; Fischer, Douglas. *As Obrigações Processuais Penais Positivas – Segundo as Cortes Europeia e Interamericana de Direitos Humanos*. Porto Alegre: Livraria do Advogado, 6ª ed, 2026.

Suxberger, Antônio Graciano. "Cadeia de custódia como meio de identificação da prova: a interseção entre a probática e a epistemologia probatória".

Cuomo, Alessandro; D'Agostino, Giuseppe; Ianulardo, Pasquale. Android forensics: limits of hash code repeatability in mobile device extractions. [S. l.: s. n.], 2022. Disponível em: https://www.researchgate.net/. Acesso em: 22 ago. 2026.

Silva, Fabrício Lamas Borges da; Wendt, Emerson. Mensagens de aplicativos de mensageria como provas no processo penal: uma análise de decisões do STJ. In: IOCOHAMA, Celso Hiroshi; RIBEIRO, Luiz Gustavo Gonçalves; CASTRO, Matheus Felipe de (org.). *Direito penal, processo penal e constituição III*: XXXI Congresso Nacional do CONPEDI, Brasília, DF. Florianópolis: CONPEDI, 2024. p. 12-31. Disponível em: https://site.conpedi.org.br/publicacoes/l23282p8/nt4j1pf1/nGFI3Dx0rF04G11d.pdf. Acesso em: 22 ago. 2026.

1 "*O fato de não existir referida ficha, por óbvio, não revela a quebra da cadeia de custódia da prova, em especial diante da expressa afirmação de que a correta custódia dos vestígios é inerente à carreira pericial. De fato, conforme afirmado pela própria defesa, a cadeia de custódia da prova não surgiu apenas com a mencionada lei, passando apenas a ser melhor sistematizada.* […] *(Agravo Regimental no Habeas Corpus n° 901.602-PB, STJ, 5ª Turma, Rel. Min. Reynaldo Soares Da Fonseca, julgado em 12.2.2025, publicado no DJ em 11.3.2025)*

2 Suxberger, Antônio Graciano. "Cadeia de custódia como meio de identificação da prova: a interseção entre a probática e a epistemologia probatória". In: Cadeia de Custódia da prova no processo penal. Paulino, Galtiênio da Cruz e outros (orgs). São Paulo: Tirant Lo Blanch, 2024, p. 23 e seguintes.

3 [...] A quebra da cadeia de custódia não configura nulidade processual, mas está relacionada à *eficácia da prova*. A defesa não comprovou adulteração da prova ou intercorrências no seu iter. 5. O relatório de investigação produzido por policiais civis é válido, pois se trata de documento descritivo que não requer expertise técnica específica. [...] Agravo regimental desprovido. *(Agravo Regimental no Habeas Corpus n° 924.130-SE, STJ,5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 12.2.2025, publicado no DJ em 25.2.2025)*

4 Pacelli, Eugênio; Fischer, Douglas. Comentários ao Código de Processo Penal e sua Jurisprudência. Salvador: Juspodivm, 2026, 18ª ed, item 563.3.