ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

META-EVIDÊNCIA DIGITAL: A DUALIDADE NA CADEIA DE CUSTÓDIA ENVOLVENDO DISPOSITIVOS ELETRÔNICOS E EVIDÊNCIAS DIGITAIS.

André Luis Fernandes[1]

Rodrigo Henrique de Oliveira Montes[2]

RESUMO

A tecnologia está cada vez mais presente em nosso dia a dia e não é diferente no ambiente jurídico. É vertiginoso o aumento da quantidade de informações digitais armazenadas em dispositivos eletrônicos, as quais estão envolvidas em procedimentos investigativos, consideradas como evidências digitais. São documentos, imagens, vídeos, áudios, qualquer tipo de informação armazenada em formato binário. Diante disso, o presente trabalho tem como objetivo apresentar as principais características que envolvem esses arquivos, e consequentemente sua manipulação, sob o enfoque da garantia da integridade de seu conteúdo. O estudo busca descrever como as evidências digitais podem e devem ser obtidas e, principalmente, a considerar a recente (2019) alteração no Código de Processo de Penal referente à cadeia de custódia, apresentar o conceito que envolve a dualidade dessa cadeia de custódia quando da manipulação das provas digitais, consideradas meta-evidências, obtidas de dispositivos eletrônicos os quais estão intrinsicamente presentes em nossa sociedade e, diante da sua importância dentro das lides processuais, há de serem manipulados de forma correta visando manter a validade do seu valor probante.

Palavras-chave: Cadeia de Custódia; Dispositivos Eletrônicos; Evidência Digital; Meta-Evidencia Digital; Prova Digital.

ABSTRACT

Technology is increasingly present in our daily lives and it is no different in the legal environment. The increase in the amount of digital information stored in electronic devices is vertiginous, which are involved in investigative procedures, considered as digital evidence. They are documents, images, videos, audios, any type of information stored in binary format. In view of this, the present work aims to present the main characteristics that involve these files, and consequently their manipulation, with a focus on guaranteeing the integrity of their content. The study seeks to describe how digital evidence can and should be obtained and,

[1] Perito Criminal da Polícia Científica de São Paulo, Professor da Academia de Polícia de São Paulo, Graduado em Computação e Direito, Pós-Graduado em Sistemas e Segurança da Informação. luis.alf@policiacientifica.sp.gov.br.

[2] Perito Criminal da Polícia Científica de São Paulo, Professor da Academia de Polícia de São Paulo, Graduado e Mestre em Química, Pós-Graduado em Investigação Criminal e Psicologia Forense e Pós-Doutorado em Química. rodrigo.rhom@policiacientifica.sp.gov.br.

mainly, considering the recent (2019) change in the Code of Criminal Procedure regarding the chain of custody, to present the concept that involves the duality of this chain of custody when the manipulation of digital evidence, considered meta-evidence, obtained from electronic devices which are intrinsically present in our society and, given their importance within procedural matters, must be handled correctly in order to maintain the validity of their probative value.

Keywords: Chain of Custody; Electronic devices; Digital Evidence; Digital Meta-Evidence; Digital Proof.

1 INTRODUÇÃO

Indubitavelmente a tecnologia presente na sociedade é ferramenta essencial e indispensável. Também é inquestionável que não se vislumbra uma existência natural sem esse arcabouço digital.

Em uma dita Sociedade da Informação, não podemos olvidar de que essa tecnologia muito nos proporciona, em todos os níveis, desde quando podemos frequentar ambiente de um supermercado sem sair do conforto do lar, até mesmo quando, em home-office, desfrutamos da companhia da família e dos animais de estimação, enquanto exercemos nossa atividade profissional, sem sequer colocar os pés colocar na rua.

O ambiente jurídico não é diferente. Ele sofre a mutação que ocorre na sociedade, criando as adequações pertinentes, independente do ramo em que estiver inserido, pois é uma ciência evolutiva que acompanha a sua sociedade.

Considerando o viés jurídico relacionado à produção de provas a ele inerentes, há uma crescente demanda na quantidade de arquivos digitais que permeiam seus procedimentos, investigativos e processuais. E esses arquivos digitais nada mais são do que documentos, porém de forma eletrônica, diferentemente dos documentos no formato físico, onde as informações são inscritas em papel e, portanto, tangíveis, os documentos eletrônicos não são palpáveis.

Não obstante esses documentos físicos possam tornar-se digitais, através de uma fotografia ou um escaneamento, ainda assim seu meio de produção é físico. Por outro lado, aqueles (eletrônicos), estão dissociados de uma plataforma física única de armazenamento.

Esses arquivos digitais por vezes trafegam armazenados entre diversos dispositivos eletrônicos – DVDs, pen-drives, HDs, plataformas remotas (*cloud storage*). Ou seja, o documento digital não está preso a um único e distinto meio físico,

Assim como ocorre com os documentos físicos em papéis, através de assinaturas e certidões que garantem a sua autenticidade e a sua integridade, aos documentos digitais não é diferente. Surge então a necessidade de garantir aos documentos digitais as mesmas garantias de veracidade da prova que existem nos documentos físicos.

Ferramentas forenses aliadas a técnicas específicas visam permear a seara tecnológica que envolve os documentos utilizados como provas nas lides judiciais, de características irrefutáveis em direção à força probante do documento digital. É imprescindível que todos os procedimentos de documentação realizados com os vestígios digitais visando a preservação de sua credibilidade em todas as etapas da persecução penal permitam a concretização dos princípios basilares do contraditório e da ampla defesa, uma vez que controlam a atuação estatal sobre aquilo que será fonte de prova.

Vislumbra-se, portanto, uma vertente específica, norteada pelo ramo do Direito Digital, visando dentre outros assuntos, o tratamento dos vestígios e provas binárias envolvendo o ambiente computacional, que, devido às suas características específicas, exige dos operadores do direito uma atenção especial na produção, recebimento, transmissão e manipulação dos conteúdos envolvendo dados eletrônicos.

2 O DIREITO E A EVOLUÇÃO DA TECNOLOGIA

Uma sociedade envolvida por indivíduos variados está em mutação e evolução constantes. Nascida em meio à Guerra Fria, a Arpanet – uma rede militar de computadores de estrutura descentralizada – dá início a uma nova era, a era da informação. Mais tarde, já nos anos 90, essa rede militar surge no meio acadêmico e comercial, nasce então a internet.

A rede mundial traz para os indivíduos a possibilidade de comunicação em massa e de forma individualizada. As pessoas passam a ter acesso às informações de forma imediata, aplicando um valor imensurável ao conteúdo presente nessa aldeia globalizada.

Acompanhando esse crescimento da velocidade da informação, os equipamentos eletrônicos evoluíram, principalmente com o surgimento dos dispositivos portáteis, como celulares, smartphones e tablets.

Não bastasse essa evolução natural, diante da nova realidade social provocada pela pandemia causada pelo vírus Covid em 2019, tanto a sociedade como a tecnologia sofreram transformações abruptas. Foi necessário evoluir muito mais rápido do que o normal, o que trouxe, e ainda traz, consequências negativas.

Segundo a especialista em direito digital Patrícia Peck Pinheiro:

> A meta do ordenamento jurídico é ser uma organização centralizada do poder que teria como vantagens a adaptabilidade diante das mudanças, o que garantiria o seu grau de certeza e eficácia na sociedade. Há, então, a participação interativa da realidade no momento de concepção da norma, havendo uma adaptação valorativa desta ao contexto social. (Pinheiro, 2015, p.35).

As relações sociais, diante dessa nova perspectiva, acabam deixando de ser diretas e passam a ser tecnológicas: comunicações por aplicativos, reuniões através de conexões remotas por computadores, aulas virtuais, acesso bancário através dos smartphones e, com isso, a realidade jurídica busca suprir as lacunas legislativas sobre o assunto.

> É certo, porém, que o Direito sendo um fenômeno cultural, deve acompanhar a realidade temporal e geográfica em que se envolve. O Direito conhece, por isso, uma inevitável servidão relativamente à realidade espacial circundante, pelo que todas as evoluções do mundo social, político e econômico condicionam ou influenciam o mundo jurídico. (Marques, 2006, p.76)

Porém sabemos que a velocidade exacerbada da evolução da tecnologia acompanhada pela sociedade, está longe de ser acompanhada pelas consequentes reações jurídicas. Nesse ínterim, operadores do direito das mais diferentes áreas devem estar atentos às divergências ou às lacunas jurídicas existentes, evitando que a sociedade fique desamparada em suas garantias e direitos, frente à avalanche tecnológica à qual está submetida.

Atualmente os processos deixaram de ser físicos, os documentos que antes estavam em papéis tornam-se, seja transferidos ou seja desde a sua origem, documentos digitais.

Acompanhando essa vertente tecnológica, a produção de provas requer cuidado especial, principalmente quando sua legitimidade está sob o crivo da tecnologia, daí a importância em mantermos uma forma válida na sua produção e manipulação.

3 VESTÍGIOS NO AMBIENTE DIGITAL

Podemos considerar o ambiente digital como aquele em que os arquivos, que consistem em registros eletrônicos em bits, estão gravados sempre em algum tipo de suporte como discos rígidos (HD) de computadores, memórias eletrônicas de smartphones ou pen drives, dentre outros. Esses registros eletrônicos são os arquivos digitais de texto, de vídeo, de áudio, de imagens, ou seja, qualquer informação armazenada em alguma plataforma eletrônica.

Conforme apresentado por Augusto Tavares Rosa Marcacini, o documento eletrônico:

> [...] não se prende ao meio físico em que está gravado, possuindo autonomia em relação a ele. O documento eletrônico é, então, uma sequência de bits que, traduzida por meio de um determinado programa de computador, seja representativa de um fato. Da mesma forma que os documentos físicos, o documento eletrônico não se resume em escritos: pode ser um texto escrito, como também pode ser um desenho, uma fotografia digitalizada, sons, vídeos, enfim, tudo que puder representar um fato e que esteja armazenado em um arquivo digital. (MARCACINI, 1999).

No direito brasileiro temos uma variedade de definições e conceitos sobre provas, seja no âmbito criminal, cível, trabalhista ou administrativo. Por certo, muitos institutos jurídicos trazem em seu bojo especificações relacionadas às provas digitais, porém sem exauri-los. Sob o aspecto penal, vale aqui o ensinamento do mestre Norberto Cláudio Pâncaro Avena:

> [...] é preciso ter em mente que a regulamentação dos meios de prova existente no Código de Processo Penal não é taxativa, podendo ser aceitos meios de provas atípicos ou inominados, vale dizer, sem regulamentação expressa em lei, amplitude esta que se justifica na própria busca da verdade real que, sempre, será o fim do processo penal (AVENA, 2017, p. 314)

Considerando que os procedimentos investigativos e judiciais devem seguir essa evolução tecnológica, os vestígios e provas também os acompanharão, ou seja, em que pese ainda muitos documentos serem físicos, seja pela historicidade da sua produção ou mesmo pela necessidade a depender da sua origem, existirá a necessidade de transformá-los em

documento digital, assim como aqueles coletados diretamente de plataformas digitais, como um vídeo produzido em um smartphone, do qual será obtido sob método específico de extração.

Não obstante as peculiaridades que envolvem as características da prova digital, ela deve, assim como os demais meios de provas, ser produzida e mantida por meios lícitos, a fim de que se preste como forma válida e irrefutável de convicção sobre os fatos alegados na lide.

O valor probatório de uma prova, seja digital ou não, está direta e intrinsecamente relacionado a, no mínimo, dois requisitos fundamentais: que possa garantir a autoria da produção do documento/arquivo – a autenticidade – e que possa garantir que seu conteúdo seja íntegro desde a sua produção – a integridade.

Garantir a autenticidade de uma prova digital significa que podemos sempre determinar e, se necessário confrontar, a sua origem de obtenção (como extrair uma imagem de um computador) ou de produção (emissão de um documento escrito em um editor de textos).

Após a obtenção ou a produção de um arquivo, é essencial que o seu conteúdo esteja protegido de adulterações, sejam elas oriundas de uma atividade ilícita, ou mesmo por um manuseio indevido, pois devido à sua sensibilidade, com muita facilidade pode ocorrer a modificação de conteúdo de arquivos digitais ou até mesmo sua destruição.

Portanto, o valor probatório da prova digital está diretamente relacionado às técnicas e ferramentas utilizadas na manipulação dessas evidências, seja da evidência de armazenamento (o dispositivo eletrônico) ou sua meta-evidência (arquivo digital armazenado).

Na vertente criminal, o artigo 158 do Código de Processo Penal é claro em afirmar que, enquanto integrante do corpo de delito, o documento (digital) deve ser submetido a exame pericial. Sob o ponto de vista cível e trabalhista, conforme artigo 373 do Código de Processo Civil e artigo 769 da CLT, as provas obtidas em meios eletrônicos possuem seus valores probantes na lide.

Considerando então que as provas em ambientes digitais, assim como todos os outros meios de provas, podem e devem estar dentre os meios probantes buscando trazer a convicção ao poder julgador, é essencial que seja garantido a integridade, a autenticidade, a legalidade e a licitude desse material.

As duas primeiras características serão detalhadas no próximo capítulo. Sob o ponto de vista da licitude, a prova que foi obtida através de uma violação das normas constitucionais – direito material, por certo não poderão ser utilizadas como fonte de convencimento do magistrado, sendo desentranhadas do processo, com exceção se favorável ao réu. Porém se essas normas foram obtidas violando regras processuais, tornam-se ilegítimas (direito processual), as quais não são invalidadas, podendo ser novamente produzidas de forma legítima.

Sob esta égide, considerando as características inerentes ao ambiente tecnológico de produção de provas, o conhecimento na produção ou manutenção desse material é essencial para evitar que incorram em situações de expurgo da prova ou a necessidade de uma nova produção, fato que, a depender da origem, muitas vezes a prova digital não é passível de recuperação ou nova produção, conforme adiante demonstrado.

4 META-EVIDÊNCIA DIGITAL - A DUALIDADE NA CADEIA DE CUSTÓDIA DAS EVIDÊNCIAS DIGITAIS

O termo meta, tem como um dos seus significados, atingir um objetivo que se almeja. Sob o contexto ora estudado, o objetivo precípuo quando se tem como evidência inicial um dispositivo eletrônico, é dele obter o seu conteúdo, ou seja, os arquivos digitais que nele estão armazenados.

Considerando que o dispositivo eletrônico, tratado como evidência inicial, a meta-evidência pode ser considerada aquela que se obtém da evidência.

A meta-evidência pode ser considerada como o resultado que se tem quando um dispositivo eletrônico – como evidência suporte – é submetido a um exame e dele são obtidos os arquivos digitais armazenados.

Segundo o artigo 158-A do Código de Processo Penal, inserido pela Lei 13.964/2019 “Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.”

Portanto, a coleta do dispositivo eletrônico como vestígio relacionado ao corpo de delito carece, a partir da sua identificação, que seja iniciada a cadeia de custódia, procedendo

a sua devida descrição, armazenamento e devida lacração. Os procedimentos para manter e documentar a história cronológica das fontes de prova devem ser seguidos por todos os que têm acesso a elas.

Conforme já descrito anteriormente, o dispositivo eletrônico presta-se como suporte de armazenamento dos outros vestígios, os arquivos digitais. Daí surge, portanto, quando os arquivos digitais são extraídos do dispositivo, uma nova identificação de vestígios e consequente coleta, motivando o início de um novo procedimento de cadeia de custódia, ou seja, que sejam descritos, armazenados e lacrados os documentos digitais extraídos.

Esse procedimento visa dar a devida legitimidade e integridade do documento digital e seu respectivo conteúdo.

Assim como todo vestígio físico – tangível – o vestígio digital, considerando sua intangibilidade, independentemente de sua fonte de obtenção, deve prezar por seu devido controle de recebimento, posse e manuseio, garantindo sua efetiva cadeia de custódia.

Em que pese grande parte da produção de provas digitais se dê em ambiente forense – através das perícias digitais, o procedimento técnico para garantir a cadeia de custódia deste tipo de documento deve ocorrer em qualquer ambiente onde ele seja utilizado. Daí a importância do conhecimento sobre esse procedimento por parte de todos os envolvidos (delegacia de polícia, ministério público, poder judiciário e causídicos) com a garantia da integridade desse tipo de vestígio ou prova, considerando suas características.

O arquivo digital carece de diferenciação com relação aos demais meios de provas, pois alguns atributos intrínsecos o tornam peculiar no seu tratamento. Dentre eles invisibilidade, volatilidade, fragilidade e dispersão (KIST, 2019, p. 115-116).

Sobre o atributo da invisibilidade, podemos fazer uma analogia ente o uso de equipamentos eletrônicos e assistir a uma peça de teatro. O que vemos na tela de um smartphone é só parte do que esse dispositivo está processando internamente, sem que o usuário veja. Diversas outras informações e arquivos estão nos bastidores do dispositivo.

A destruição definitiva - intencional ou não - de uma informação armazenada em um dispositivo está diretamente relacionada à característica da volatilidade. Diante de um procedimento falho, é possível que aquela informação de interesse desapareça, não sendo possível a sua recuperação, como os arquivos que permanecem na memória RAM somente enquanto o equipamento estiver ligado.

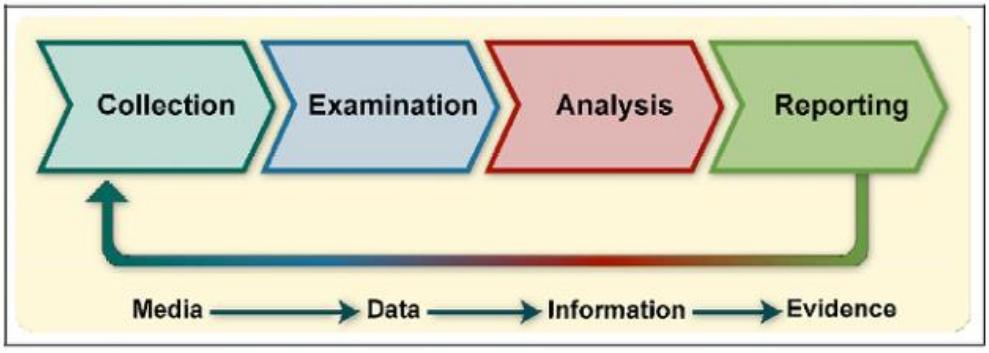
Sob o ponto de vista da fragilidade, os arquivos digitais podem facilmente ter seu conteúdo modificado, sem sequer identificar a sua adulteração, seja ela realizada por pessoas ou pelo próprio equipamento.

Por fim a dispersão tem relação direta com a diversidade de locais onde o documento digital pode estar armazenado. Cópias do mesmo arquivo ou suas partes ou complementos podem ser encontrados em um dispositivo de armazenamento físico, como um HD, e em ambiente virtual, como por exemplo as plataformas remotas de armazenamento *cloud-storage* (nuvem).

Diante dessas e outras características, é salutar que os procedimentos de manuseio desse tipo de evidência sejam realizados de forma correta evitando que sua confiabilidade seja questionada, prezando principalmente pela integridade e autenticidade dessa evidência.

Dentre alguns procedimentos e técnicas forenses indicados para referido manuseio, o NIST-National Institute Standards of Technology, definiu através da publicação SP-800-86, que esse processo deve ocorrer em quatro etapas: coleta, exame, análise e resultado.

Figura 1 – Fluxo de tratamento da evidência digital.



Fonte: National Institute Standards and Technology (2006)

A primeira fase realiza-se a coleta do material inerente ao fato, com identificação, registro, armazenamento e consequente início da cadeia de custódia. Considerando tratar-se de dispositivo eletrônico de armazenamento, a segunda fase realiza-se, através de ferramentas e técnicas forenses, a extração dos dados armazenados. A análise é a fase onde, após os dados obtidos, inicia-se o processo de fazer o relacionamento desses dados com o contexto do caso apurado. Identificadas as informações inerentes ao fato, finaliza-se o processo com o registro

desses dados em um documento formal, por exemplo, um relatório ou laudo, que constará a descrição dos procedimentos realizados e as ferramentas e técnicas aplicadas.

Destaca-se que a cadeia de custódia se inicia na fase de coleta, seja do dispositivo eletrônico ou seja do conjunto de dados digitais. Portanto é nesse momento deve-se além de produzir o documento pertinente, proceder ao lacre no que fora coletado, pois "o valor probante do documento eletrônico deve ser sempre aferido no ambiente em que ele foi gerado" (RINALDI, 2016, p. 638).

Diante das etapas demonstradas, percebe-se que a cadeia de custódia não é uma carta de recomendação, mas sim um procedimento cautelar preparatório que, obrigatoriamente, deve ser seguido para evitar nulidades no processo. Desta forma, deve-se garantir que a prova colhida é a mesma da prova valorada e, assim, a confiabilidade e a credibilidade dos arquivos digitais coletados serão preservadas.

Sob o ponto de vista de dispositivos físicos, o procedimento de lacração é permeado pela embalagem plástica, que após fechada, lhe é aplicada, de forma a garantir a integridade do conteúdo, uma fita plástica com numeração específica, conhecido como lacre. O lacre deve impedir o manuseio do vestígio por pessoas não autorizadas e visa garantir a integridade do material.

O mesmo procedimento de proteção de conteúdo deve ser igualmente aplicado face aos arquivos digitais. Em que pese esses arquivos estarem em um dispositivo lacrado, o conteúdo do arquivo se difere daquele, quando dali é extraído.

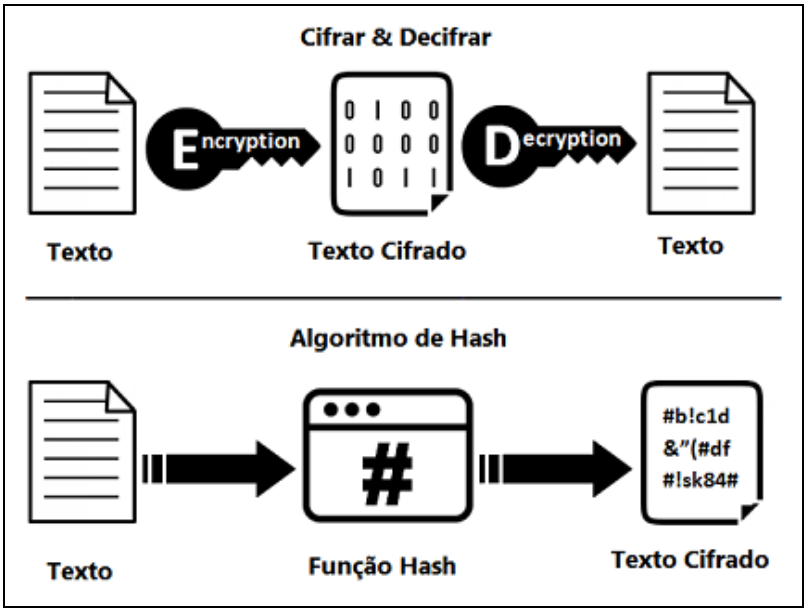
Diante da intangibilidade do arquivo digital, a técnica utilizada que visa garantir o seu conteúdo, é conhecida como resumo hash (*message-digest*).

> Uma função de hash criptográfico, muitas vezes é conhecida simplesmente como hash – é um algoritmo matemático que transforma qualquer bloco de dados em uma série de caracteres de comprimento fixo. Independentemente do comprimento dos dados de entrada, o mesmo tipo de hash de saída será sempre um valor hash do mesmo comprimento. (DONOHUE, 2014).

Ainda, segundo NIST SP-800-86, o cálculo do hash pode ser usado para verificar e garantir a integridade dos dados de um arquivo. O hash identifica o conteúdo de forma exclusiva, e, caso o conteúdo seja alterado em um único bit e um novo código hash seja gerado, esse será completamente diferente daquele. (NIST, 2003).

Convém aqui fazer a distinção do cálculo de função hash e função de criptografia. A função hash visa garantir a integridade do conteúdo do arquivo digital. Por outro lado, a criptografia permite criar autenticidade e confidencialidade ao arquivo digital. Portanto são conceitos tecnológicos que se complementam. A autenticidade é garantida quando se confere que o autor do documento é mesmo quem diz ser. A confidencialidade é conferida pois somente quem tem uma chave de acesso específica poderá conhecer o conteúdo daquele arquivo. Abaixo uma imagem que exibe a diferença básica entre os conceitos.

Figura 2 – Esquema de funcionamento de criptografia e algoritmo hash.



Fonte: iMasters[3]

Se durante a coleta de um arquivo digital, gerar um resumo do seu conteúdo com a função hash, este retorna um valor, composto por letras e números, de tamanho específico a depender do tipo de hash utilizado. Por exemplo, considere um arquivo texto que seu conteúdo é composto por "DIREITO-E-TI". Ao submeter tal conteúdo ao algoritmo de função hash tipo SHA256 teremos como resultado a expressão "5f4017721a09992053dd91a78d28abcbda5ff3259be9f299bfe0d8a793199a6f". Em seguida, alterando o conteúdo para "DIREITO E TI", e submetendo novamente o mesmo arquivo de

[3] https://imasters.com.br/dotnet/criptografia-na-plataforma-net (acesso em 19 set 2022).

texto à mesma função hash tipo SHA256 o resultado será "2b97d6c267f456ef1160af83eee5b8875faf91a7c23b62a2bb5ef663a5c94969".

Através da chave hash não é possível identificar o conteúdo do arquivo origem e nem o que foi nele modificado. A chave hash vai garantir que, se for diferente, certamente o conteúdo do arquivo de origem foi adulterado, tornando aquela evidência digital uma prova a ser questionada quanto à sua integridade, padecendo de nulidade, semelhante à violação do lacre ou da embalagem que armazena uma evidência material.

Diante dessa violação da cadeia de custódia, ensina o mestre Manuel Monteiro Valente (2020, p.77) haverá, por conseguinte, o desentranhamento da evidência, diante da inadmissibilidade de sua valoração que resulta na proibição do seu uso no arcabouço probatório.

Ainda sob esse aspecto da quebra da cadeia de custódia Lopes Junior afirma que "sem dúvida deve ser a proibição de valoração probatória com a consequente exclusão física dela e de toda a derivada" (2017, p. 414).

É notória a importância da preservação do vestígio desde a sua coleta até o seu descarte, principalmente, conforme visto acima, quando tais vestígios possuem características que os diferem dos demais, exigindo uma atenção especial por parte daqueles que os manuseiam.

5 CONSIDERAÇÕES FINAIS

Diante do mundo tecnológico em que vivemos, não podemos fechar os olhos frente às mudanças que isso acarreta no mundo jurídico.

A identificação dos vestígios e consequente produção de provas é ponto essencial na lide processual. O elemento probatório é aquele em que as partes do processo devem estabelecer, de forma irrefutável, os elementos que subsidiarão a decisão do Estado-Julgador.

Sob esta égide, discorre o mestre Aury Lopes Junior:

> O tema de provas exige a intervenção de regras de 'acreditação', pois nem tudo que ingressa no processo pode ter valor probatório; há que ser 'acreditado', legitimado, valorado desde sua coleta até a sua produção em juízo para ter valor probatório. (LOPES JUNIOR, 2017, p. 412).

Em que pese tratarmos de arquivos baseados em bits, para que esses arquivos, neste estudo também chamados de documentos eletrônicos, possam apresentar força probante, devem carregar consigo basicamente duas características principais: a autenticidade e a integridade. A autenticidade garantindo sua origem de produção e a integridade demonstrando que não há modificação do seu conteúdo.

> Vale destacar que tais parâmetros – autenticidade e integridade – são expressamente previstos pela legislação processual para o registro de atos processuais eletrônicos (art. 195 do Código de Processo Civil8) e podem ser estendidos, seja por analogia, seja pela própria finalidade da prova, a todo e qualquer registro eletrônico que se pretenda utilizar com força probante no processo. (PASTORE, 2020, p. 68).

A manutenção dessas duas características visa legitimar, desde a coleta dos vestígios, até a sua transformação em prova. Esse caminho a ser percorrido pelo material probante está diretamente vinculado à correta manipulação da cadeia de custódia.

Tanto a importância da sua correta manipulação, que o artigo 158B, incluído no Código de Processo Penal (Decreto-lei no 3.689/1941) através da Lei 13.964/2019, traz dez etapas a serem aplicadas para que o rastreamento do vestígio seja realizado de forma segura, e seu fiel cumprimento garante a licitude do material probante.

A segurança na manipulação dos vestígios, disposta nos procedimentos previstos no citado artigo, não deve ficar restrita ao ramo processual penal, mas também aplicada aos demais ramos processuais do direito brasileiro.

Diante do que apresentamos até aqui, não há como, aos operadores do direito, que buscam a produção lícita e legítima da prova nos autos processuais, desconhecerem os procedimentos válidos que permeiam esse objetivo, desde a identificação do vestígio até o seu descarte.

No que se refere aos vestígios baseados em dispositivos eletrônicos e sua meta-evidência digital, ou seja, os arquivos digitais nele armazenados, as suas características, anteriormente já apresentadas, exigem uma atenção especial, haja vista que qualquer indivíduo, até crianças, possui razoável conhecimento sobre como manipular, por exemplo, um smartphone e os arquivos que ele armazena.

Portanto saber como tratar um equipamento eletrônico envolvido em alguma lide, para que ele, e seus arquivos, não sejam considerados posteriormente provas invalidadas, buscou-

se com esse estudo apresentar uma forma simples e clara para minimizar futuros prejuízos processuais.

REFERÊNCIAS

ALVES, M. Como escrever teses e monografia: um roteiro passo a passo. Rio de Janeiro: Elsevier, 2007.

AVENA, Norberto Cláudio Pâncaro. Processo Penal / Norberto Avena . – 9ª ed. Rev. E atual. – Rio de Janeiro: Forense; São Paulo: Método, 2017.

CERVO, Amado Luiz. **Metodologia científica**. In Amado Luiz *Cervo*, Pedro Alcino Bervian, Roberto da *Silva*. -- 6. ed. --. São Paulo: Pearson Prentice Hall, 2007.

DONOHUE, Brian. Hash: o que são e como funcionam. **Kaspersky Daily**, 10/04/2014. Disponível em: https://www.kaspersky.com.br/blog/hash-o-que-sao-e-como-funcionam/2773/. Acesso: 19 set. 2022.

KIST, Dário José. **A prova digital no processo penal**. Leme: JH Mizuno, 2019.

LOPES JUNIOR, Aury. **Direito Processual Penal**. 14ª. ed. São Paulo: Saraiva, 2017.

MARCACINI, Augusto Tavares Rosa. **O documento eletrônico como meio de prova**. 1999. Disponível em: simagestao.com.br/wpcontent/uploads/2016/05/Odocumentoeletronicocomomeiodeprova.pdf. Acesso em: 26 abr. 2022.

MARQUES, Garcia; MARTINS, Lourenço. **Direito da Informática**. 2. ed. Coimbra: Almedina, 2006, p.76.

NATIONAL INSTITUTE STANDARDS AND TECHNOLOGY. Guide to integrating forensic techniques into incident response. **NIST Special Publication 800-86**. Gaithersburg: NIST, 2006. Disponível em: csrc.nist.gov/publications/detail/sp/800-86/final. Acesso em: 19 set. 2022.

PASTORE, Guilherme de Siqueira. Considerações sobre a autenticidade e a integridade da prova digital. **Cadernos jurídicos / Escola Paulista da Magistratura**. Imprenta: São Paulo, Escola Paulista da Magistratura, 2000. v. 21, n. 53, p. 63–79, jan./mar., 2020. Disponível em: bdjur.stj.jus.br/jspui/handle/2011/142286. Acesso em: 27 set. 2022.

PINHEIRO, Patricia Peck. **Direito digital**. 2ª. ed., 2ª. tir., rev. atual. ampl. São Paulo: Saraiva, 2008.

PINHEIRO, Patricia Peck. **Direito digital** — 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737 de 2012 — São Paulo: Saraiva, 2013.

RINALDI, Luciano. Dos documentos eletrônicos (arts. 439 a 441). *In*: CABRAL, Antonio do Passo; CRAMER, Ronaldo (coord.). **Comentários ao novo Código de Processo Civil**. 2. ed. Rio de Janeiro: Forense, 2016.

VALENTE, Manuel Monteiro Guedes. **Cadeia de custódia da prova**. 2. ed. Coimbra: Almedina, 2020.