A TECNOLOGIA BLOCKCHAIN COMO FERRAMENTA VIÁVEL PARA CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS

Heloísa Daniela Nora[1]
Cinthia Obladen de Almendra Freitas[2]

Recebido em 12/06/2024
Aceito em 18/12/2024

RESUMO
Os fatores no cenário da sociedade contemporânea se conectam no contexto de uma sociedade informacional, que altera a forma e a velocidade com que a mudança impacta os indivíduos. Nesse contexto frenético, está o Direito Penal, que tenta acompanhar as novas práticas delitivas que surgem com essa transformação, afetando inclusive as evidências deixadas nas cenas de crime, que demandam uma abordagem diferenciada em relação à cadeia de custódia. Diante desse cenário, percebe-se a necessidade de unir a tecnologia e o Direito para lidar de forma efetiva com a velocidade das transformações que ocorrem. O artigo tem como objetivo conceituar a prova digital, incorporá-la à cadeia de custódia e fazer a aplicação dos conceitos desenvolvidos na tecnologia Blockchain com a finalidade de responder à seguinte pergunta: a cadeia de custódia da prova digital pode ser realizada por meio da implementação da tecnologia Blockchain? Como hipótese, se estabeleceu que a tecnologia Blockchain se mostra como uma alternativa viável para a cadeia de custódia das provas digitais. Para alcançar seus resultados, adotou-se metodologia hipotético-dedutiva com revisão e levantamento bibliográfico. Os resultados demonstraram que as características da tecnologia Blockchain oferecem uma ferramenta viável para realizar o procedimento da cadeia de custódia de forma transparente..

PALAVRAS CHAVE: *blockchain*; cadeia de custódia; novas tecnologias; provas digitais; sociedade informacional.

BLOCKCHAIN TECHNOLOGY AS A VIABLE TOOL FOR CHAIN OF CUSTODY OF DIGITAL EVIDENCES

ABSTRACT
The factors in the contemporary societal landscape connect within the context of an informational society, which alters how change impacts individuals in terms of both form and speed. Within this frenetic context lies Criminal Law, which seeks to keep pace with emerging criminal practices brought about by this transformation, affecting even the evidence left at crime scenes, necessitating a specialized approach to chain of custody. Considering this scenario, the need to merge technology and law to effectively manage the speed of these transformations becomes apparent. The article aims to conceptualize digital evidence, integrate it into chain of custody, and apply Blockchain technology to answer the question: can the chain of custody of digital evidence be achieved through the implementation of Blockchain technology? The hypothesis established is that Blockchain technology proves to be a viable alternative for the custody of digital evidence. To achieve

[1] Mestranda pelo Programa de Pós-Graduação em Direito (PPGD) da Pontifícia Universidade Católica do Paraná (PUCPR), bolsista CAPES.
[2] Mestre em Engenharia Elétrica e Informática Industrial pela Universidade Tecnológica Federal do Paraná (1990) e Doutora em Informática pela Pontifícia Universidade Católica do Paraná (2001). Professora Titular da Escola de Direito da PUCPR e Professora Permanente do Programa de Pós-Graduação (Mestrado/Doutorado) em Direito (PPGD) da PUCPR.

its results, a hypothetico-deductive methodology was adopted, including literature review and data collection. The results demonstrated that the characteristics of Blockchain technology offer a viable tool for conducting chain of custody procedures transparently.

Keywords: blockchain; chain of custody; digital evidence; informational society; new technologies.

1 INTRODUÇÃO

O advento tecnológico impactou as relações sociais e está redefinindo profundamente a sociedade moderna, impactando também, no campo jurídico. Autores como Manuel Castells (2005), Klaus Schwab (2016) e Byung-Chul Han (2022) destacam a emergência de uma sociedade informacional, na qual o poder está intimamente ligado ao controle e acesso à informação. A quarta Revolução Industrial, descrita por Schwab (2016), ressalta a velocidade, amplitude e impacto sistêmico das mudanças tecnológicas, enquanto Han (2022) introduz o conceito de Infocracia, pela qual o poder deriva da manipulação de informações.

Todos esses fatores se interligam no contexto da sociedade informacional que remodelou a forma e a velocidade com que a mudança impacta a vida dos indivíduos. Vivencia-se uma nova realidade em que a informação é sinônimo de fonte de poder, uma vez que, tudo se conecta pela informatização. Empresas, pessoas naturais, organizações não governamentais e, até mesmo, o Estado devem mudar a forma com que agem diante desse novo contexto. E ao seu ritmo, o Direito e o Processo Penal tentam seguir em lentos passos a transformação que assola a contemporaneidade.

Frente a um cenário de evolução tecnológica que impacta até mesmo as relações estatais, o que se observa é que há modificações, inclusive, na prática delitiva, passando a incorporar meios tecnológicos para sua instrumentalização ou até mesmo como objeto jurídico. Crimes que passam a ser cometidos envolvendo a tecnologia em seu processo consumativo acompanham esse desenvolvimento e o emprego da tecnologia nos delitos em geral, gera repercussão no âmbito processual penal, de modo que, os elementos indiciários extraídos de dispositivos tecnológicos são dotados de natureza totalmente distinta dos vestígios materiais físicos, como um projétil deflagrado ou marcas de lesões corporais, demandando, inclusive, uma abordagem especial em matéria de cadeia de custódia, ensejando tratamento distinto em relação às evidências comuns.

Tendo em vista que, os dados e informações extraídos de dispositivos tecnológicos não podem ser tratados da mesma forma com que os indícios físicos, sua coleta, acondicionamento e registro são extremamente voláteis se realizados de forma inadequada, sendo necessária a adoção de mecanismos tecnológicos seguros para cumprimento das disposições que regem a cadeia de custódia, momento em que se visualizou a probabilidade de aplicação da tecnologia *Blockchain*, tecnologia esta que tem como características sua imutabilidade e transparência.

Diante deste cenário fático, adotou-se a metodologia hipotético-dedutiva com revisão e levantamento bibliográfico, trabalhada a partir da seguinte pergunta de pesquisa: a cadeia de custódia da prova digital pode ser realizada por meio da implementação da tecnologia *Blockchain*?

Como hipótese, se estabeleceu que a tecnologia *Blockchain* se mostra como uma alternativa viável, para a cadeia de custódia das provas digitais. Desta forma, o objetivo geral preza por conceituar a prova digital, incorporá-la à cadeia de custódia e, por fim, fazer a aplicação dos conceitos desenvolvidos na tecnologia *Blockchain.*

Para alcançar os resultados, o trabalho foi estruturado da seguinte forma: inicialmente, apresenta-se o conceito e as características das provas digitais na sociedade informacional. Em seguida, discute-se a importância da cadeia de custódia para a preservação de evidências, abordando seus desafios no contexto das provas digitais. Posteriormente, introduz-se a tecnologia *Blockchain* e sua aplicação prática na cadeia de custódia, analisando como suas características podem garantir a integridade e autenticidade das provas. Por fim, são apresentados os resultados, que indicam o alinhamento das funcionalidades da *Blockchain* com os requisitos da cadeia de custódia, seguidos das considerações finais que reforçam sua viabilidade como ferramenta transformadora para o Direito Penal.

SOCIEDADE INFORMACIONAL E O DIREITO PENAL

Os instrumentos utilizados pelo Direito sempre irão refletir a sociedade em que estão inseridos. Portanto, à medida que, a sociedade enfrenta o desenvolvimento de novas tecnologias, seus impactos no campo jurídico são inafastáveis, assim como suas consequências. Segundo Castells vive-se em uma Sociedade Informacional[3], interconectada por redes invisíveis que abrangem uma vasta quantidade de dados sendo compartilhados, armazenados e processados constantemente, um dos aspectos que tornam a revolução tecnológica tão singular: a maneira como lida com as informações que gera e coleta (CASTELLS, 2005).

Sobre a Sociedade Informacional, é importante trazer o ponto de vista levantado por Boff *et al.* (2018) de que essa sociedade indica uma organização social onde a geração, processamento e transmissão de informações se convertem em fontes de produtividade e poder. Isto é, dados geram informação, que geram conhecimento – e conhecimento, muitas vezes, leva ao poder, como bem trazido pelos autores, quando conceituam o Estado informacional como uma figura que "Utiliza o controle sobre a informação para produzir e reproduzir o poder e conquistar áreas de influência autônoma no ambiente em rede" (BOFF *et al*., 2018, p. 19). Essas mudanças não se refletem apenas

[3] Ou Sociedade da Informação.

na economia, que passa ser informacional e global, mas também, no Estado como ente soberano.

Essas noções se conectam às visões de Schwab (2016) sobre a quarta Revolução Industrial. Enquanto Boff *et al.* (2018) demonstram a aplicação desse contexto informacional, dentro da figura do Estado e, Castells (2005) descreve a interconexão impulsionada pelas redes de informação. Schwab (2016) destaca como a fusão de tecnologias digitais, físicas e biológicas transforma fundamentalmente a maneira que se vive dentro da sociedade moderna. Ambos, reconhecem a natureza disruptiva das mudanças tecnológicas e sua capacidade de remodelar estruturas sociais, econômicas e políticas.

Nas palavras de Schwab (2016, p. 24): "A escala e a amplitude da atual revolução tecnológica irão desdobrar-se em mudanças econômicas, sociais e culturais de proporções tão fenomenais que chega a ser quase impossível prevê-las". Enquanto, Castells (2005) enfatiza a emergência de uma sociedade centrada na informação, Schwab (2016) destaca a convergência de tecnologias emergentes que impulsionam uma nova era.

Interessante notar que, Schwab (2016, p. 15-16) destaca 03 (três) características fundamentais da nova fase da vida em sociedade, a quarta revolução industrial, quais sejam: a velocidade; a amplitude e o impacto sistêmico. Essas características, além de auxiliar no entendimento da problemática da pesquisa, também ressoam com a análise de Castells (2005).

A primeira característica, velocidade, refere-se à rapidez com que as mudanças tecnológicas estão ocorrendo e se disseminam globalmente, impulsionando transformações rápidas e constantes em todos os aspectos da vida. A segunda, amplitude, destaca a extensão e abrangência dessas mudanças, afetado múltiplos setores e aspectos da sociedade, desde a economia até a cultura e política. Por fim, o impacto sistêmico, destaca como essas mudanças estão interconectadas e interdependentes, gerando efeitos cascata, que permeiam todo o tecido social. Juntas, essas características ressaltam a urgência de uma compreensão adaptativa das implicações dessas transformações, para enfrentar os desafios e aproveitar as oportunidades da era digital.

Byung-Chul Han (2022), filósofo sul-coreano, de expressão alemã, traz o entendimento de um regime de informação e como as informações processadas por algoritmos determinam processos sociais, políticos e econômicos (HAN, 2022). A forma de governo nomeada pela expressão que dá nome a sua obra, Infocracia, descreve uma forma de poder que se baseia na acumulação e no controle das informações por meio da vigilância e manutenção de dados pessoais. Novamente, o autor traz as ideias que também são discutidas por Boff *et al*. (2022) quando diz que a posse de informações, nessa nova sociedade, impacta diretamente no poder adquirido (HAN, 2022).

Ao observar e entender o contexto disruptivo no qual se encontra a sociedade moderna hoje, com todas as classificações expostas, surge a necessidade que se pense em uma coexistência entre a sociedade e a tecnologia, como bem pontua Schwab (2016). Com isso em mente, há de se imaginar

como essas tendências podem ser incorporadas ao Direito Penal. As três características da nova fase que a sociedade moderna se insere, trazidas por Schwab (2016), têm implicações significativas no meio criminal.

A rápida evolução do meio digital tem levado à emergência de crimes cibernéticos que exigem respostas ágeis e eficazes por parte das autoridades. Não somente isso, mas o impacto sistêmico dessas transformações, também influencia a coleta, armazenamento e análise de evidências digitais em processos criminais. Essa relação é um aspecto que se encontra na análise de Castells (2005), quando argumenta que as redes de comunicação digital reconfiguram não apenas a economia e a cultura, mas também, as estruturas de poder e controle social.

Dessa forma, a ideia de que o direito deve acompanhar a sociedade e a rápida evolução tecnológica não apenas confere novos métodos de investigação, mas também, novos métodos de cometer crimes. Embora, o direito penal seja frequentemente caracterizado por sua rigidez e procedimentalismo, não está imune às transformações sociais, como se verá a seguir. A velocidade, amplitude e impacto sistêmico dessas mudanças ressaltam a urgência de uma compreensão adaptativa das implicações legais e éticas. No entanto, enquanto, a tecnologia avança, o direito muitas vezes luta para acompanhar esse ritmo.

A crescente digitalização da sociedade moderna implica na geração constante de dados que podem servir como evidências em investigações criminais. A natureza das provas digitais muitas vezes armazenadas em dispositivos eletrônicos, apresenta desafios específicos em relação à sua autenticidade, integridade, admissibilidade, valor probatório e até mesmo definição jurídica. Por isso, após essa exposição, por meio da qual se buscou trazer o contexto das revoluções tecnológicas, passa-se a analisar as provas digitais para compreender o seu conceito no ordenamento jurídico brasileiro.

CONCEITO E CARACTERÍSTICAS DE PROVAS DIGITAIS NA SOCIEDADE INFORMACIONAL

A dinâmica de mudanças não lineares e constantes que a humanidade enfrenta reverberam na investigação criminal e identificação de vestígios probatórios. O Código Penal Brasileiro adota o modelo inquisitório, em que o processo é visto como uma forma de alcançar a "verdade real" (PRADO, 2014). Sobre esse tema, é importante trazer que o modelo inquisitório adotado pelo sistema jurídico brasileiro, é de natureza contraditória e complexa. Grande parte da doutrina defende que os modelos acusatórios e inquisitórios seriam meramente históricos, isso porque, não há como classificar um modelo na sua forma pura. Para Aury Lopes Junior (2019, p. 499), essa conceituação é utilizada como uma "maquiagem conceitual", sendo que, o autor conceitua o sistema brasileiro como *neoinquisitório*, isso porque, ainda que, sua constituição seja acusatória (com princípios como presunção de inocência

e garantia de jurisdição), há traços de um sistema inquisitório, onde a intervenção do magistrado se justifica pela busca pela "verdade real".

A qualidade de "verdade real", por sua vez, também é um tema em discussão, a busca pela verdade é algo muito relativo e a ideia de chegar em uma narrativa fiel aos fatos ocorridos é quase utópica. O mito da verdade real, é criticado por Khaled Júnior (2016), em sua obra, na qual critica a visão inquisitória do acusado como meio de prova e não como sujeito de direito. O tema é palco de debate, mas não coube aprofundar essa discussão nesse estudo. Por mais que seja relevante, é importante que se entenda que a busca da verdade processual, diferente da verdade real, pode ser alcançada por meio da somatória de vestígios deixados pelo fato delituoso.

Visto isso, é possível afirmar que a produção de provas é o meio pelo qual se verifica a veracidade, mesmo que não total, dos fatos ilícitos ocorridos. O Código de Processo Penal (BRASIL, 1941), entre os artigos 158 e 250, prevê as espécies de prova, a fim de que, se emita um juízo de valor, comprovando autoria e materialidade, mas o código não faz menção às provas digitais, que são a forma de comprovar autoria e materialidade de um crime ocorrido no ambiente digital, como seu próprio nome preconiza.

Lopes Junior (2019) traz em sua obra, que o intento do processo penal, observadas as lógicas utilizadas pelo maquinário judiciário, é o de reconstruir de forma aproximada fatos que já ocorreram. O juiz irá realizar uma atividade cognitiva se baseando na peça acusatória e, para isso, precisa de provas hábeis a produzir seu conhecimento, que servirá de embasamento para a sentença proferida.

Diante das mudanças trazidas por uma transformação tecnológica acelerada e globalizada, que possibilitou o aumento da criminalidade cibernética e a transnacionalidade dos delitos cometidos por meio da Internet, houve a necessidade de uma resposta coordenada e eficaz por parte das nações. Nesse contexto, a Convenção de Budapeste (BRASIL, 2023) emergiu como um marco importante na busca por soluções jurídicas e operacionais, para combater o cibercrime em uma escala internacional. Proposta pelo Conselho da Europa, em 2001 e em vigor desde 2004, essa convenção foi o resultado de esforços para estabelecer padrões comuns, promover a cooperação entre os países e fortalecer a capacidade de enfrentamento aos desafios impostos pela era digital.

A Convenção (2023) estabelece um conjunto de princípios e procedimentos que visam facilitar a prevenção, investigação e punição dos crimes cibernéticos, além de, promover a cooperação internacional e proteção de direitos humanos no ambiente digital. Em 2023, o Brasil tornou-se parte dos países que aderem ao instrumento internacional por meio do Decreto nº 11.491 (BRASIL, 2023) o qual traz a decisão publicada no Diário Oficial da União. Dividida em quatro capítulos[4], traz um

[4] Os capítulos são: (I) Utilização de terminologias; (II) Medidas a serem implementadas a nível nacional; (III)

conceito interessante em seu artigo primeiro, letra 'b', referindo-se a "dados de computador":

> b. "dado de computador" é qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador que inclua um programa capaz de fazer o sistema realizar uma tarefa (BRASIL, 2023);

A expressão dados de computador é citada cerca de trinta vezes durante todo o texto, tanto nos primeiros artigos quanto ao final do documento. Mas seria essa expressão, então, a definição legal de uma prova digital?

Segundo Badaró (2021, *on-line*) os elementos de prova relevantes, em um contexto de Computação Forense são aqueles: "[...] conservados e transmitidos em linguagem não natural, mas digital". Nesse mesmo sentido, PIRATELLI; FREITAS, 2022, p. 16-17) conceituam as provas digitais como: "Provas digitais são, portanto, evidências digitais que podem ser coletadas e analisadas por métodos e técnicas de Computação Forense, visando a partir de hipóteses obter inferências válidas". E, há que se considerar que as provas digitais possuem 03 (três) características que as diferem de outros meios de prova: volatilidade, ubiquidade e dispersão (BADARÓ, 2021).

Vaz (2012 p. 64) conceitua a prova digital como os "dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação os quais contém a representação de fatos ou ideias". Essa definição dada às provas digitais não comportam as provas documentais, segundo Vaz (2012), ainda que utilizem informações decorrentes do meio digital (como aqueles documentos obtidos por terceiros através de uma requisição, por exemplo), isso porque, não é o formato que vai definir a natureza da prova e, sim o arquivo informático. Também não se entendem como prova digital os dados bancários, por exemplo, obtidos mediante busca e apreensão. A peculiaridade da prova digital está exatamente na forma de arquivamento da informação, que leva a procedimentos especiais na obtenção e produção da prova e não pode ser confundida com a prestação de informações em formato digital.

Na doutrina internacional a prova digital é definida por Casey (2004), como qualquer dado armazenado ou transmitido usando um computador que confirma ou rejeita uma teoria a respeito de como ocorreu um fato ofensivo ou que identifica elementos essenciais da ofensa como intenção.

O que se pode retirar, em primeiro momento, é que a prova digital se insere no gênero maior de prova científica e para que a coleta, manipulação e tratamento de vestígios dessa natureza sejam bem-sucedidos, a operação deve guiar-se por critérios e métodos científicos, que requerem que a pessoa responsável pelo procedimento seja dotada de qualificação para tanto (BADARÓ, 2021). Ainda, extrai-se que a prova digital se diferencia de documentos ou evidências obtidas de forma eletrônica exatamente por sua forma de arquivamento.

Cooperação Internacional; (IV) Disposições finais.

Badaró (2021, *on-line*) também traz em seu artigo os *standards* técnicos, da série ISO/IEC 27000[5] (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2018), destacando a ISO/IEC 27035:2011, ISO/IEC 2741:2015 e a ISO/IEC 27042/2015. Do ponto de vista operacional, é interessante adotar as normas editadas pela ISO/IEC já que não há enquadramento legislativo para as provas digitais, por mais que não sejam obrigatórias, essas normas servem como um padrão e referência para a área de Segurança da Informação, utilizadas, inclusive, pela perícia forense digital e reconhecidas internacionalmente (FURLANETO; SANTOS, 2020).

A norma técnica ABNT NBR ISO/IEC 27037:2013 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013) traz diretrizes para identificação, coleta, aquisição e preservação de evidência digital, dentre outros pontos debatidos, traz três pilares fundamentais presentes em todas as evidências digitais: a relevância, isto é, a evidência digital é considerada relevante quando se destina a provar ou refutar um elemento de um caso específico sendo investigado; a confiabilidade, referindo-se a sua correspondência com a original e, por fim, a suficiência, que diz respeito a capacidade da evidência de responder as questões levantadas com integridade e adequabilidade (OLIVEIRA, 2018).

Quanto as suas características, Kist (2019, p. 118) enumera como propriedades das provas digitais: fragilidade, dispersabilidade, volatilidade e incorporeidade. A dispersão, nesse caso, pode ser criticada, afinal, não é característica comum a toda prova digital, por exemplo: em uma investigação pode ser possível encontrar o objeto de interesse em apenas um dispositivo ou somente um arquivo. Para elucidar a questão, utiliza-se das características das provas digitais elencadas por Vaz (2012 p. 67-70), sendo elas: imaterialidade, volatilidade, facilidade na clonagem e dispersão, e a indispensabilidade de dispositivo acessório necessário à sua transmissão.

A imaterialidade da prova digital impede seu manuseio físico e permite o armazenamento de grandes quantidades de dados sem ocupar espaço físico significativo. A volatilidade, decorrente dessa imaterialidade, torna os dados frágeis e suscetíveis a alterações ou desaparecimentos com pequenas mudanças. A suscetibilidade à clonagem, também derivada da imaterialidade, permite a criação de infinitas cópias, dificultando a identificação de um original. Já a intermediação por meio físico é indispensável, pois apenas equipamentos podem tornar as sequências numéricas compreensíveis para os humanos.

Visto isso, é possível chegar a uma resposta quanto à primeira questão formulada sobre os dados de computador elencados pela Convenção de Budapeste (2023). Sim, a definição, por mais ampla, engloba as provas digitais, o que representa um avanço para a definição da prova digital nesse

[5] Esses parâmetros internacionais foram publicados pela *International Organization for Standardization* (ISO) e pela *International Electrotechnical Commission* (IEC).

sentido. Entretanto, o que não pode deixar de se notar é a negligência legislativa quanto a problemática da prova digital, afinal, suas peculiaridades demandam procedimentos especiais e específicos para a realização dos procedimentos correspondentes, principalmente, à cadeia de custódia. A manipulação (feita de forma consciente ou não) da prova digital de forma inadequada pode acarretar a imprestabilidade da prova no conjunto probatório, prejudicando o exercício da defesa ou uma apreciação incorreta dos fatos.

Assim, é possível identificar como a prova digital expande o conceito de prova documental, para incluir em sua classificação as informações e dados eletrônicos armazenados em dispositivos digitais. As características elencadas influenciam diretamente nos métodos utilizados para preservar a integridade das provas digitais, tornando-as instrumentos aptos para auxiliar na reconstrução dos fatos ocorridos em um processo penal. Além disso, suas particularidades exigem procedimentos especiais para conduzir os processos relacionados à cadeia de custódia, que serão discutidos no próximo tópico.

A CADEIA DE CUSTÓDIA E A PROVA DIGITAL

Em um caminho em busca da verdade, é possível perceber ser praticamente impossível retornar ao passado para analisar exatamente o que aconteceu. O que se consegue são vestígios, fragmentos de um todo. A soma desses fragmentos pode ou não, nos levar a uma resposta. Mesmo pessoas que testemunham os eventos captam apenas um ponto de vista da situação, com uma visão limitada do ocorrido (BRETAS, 2017). Na sociedade informacional, a quantidade de informações que podem ser utilizadas para traçar um caminho e formar uma *opinio delicti* muda bruscamente a forma que essa busca é realizada.

Entretanto, não é apenas coletar informações e somá-las para chegar em uma verdade correspondente. Isto é, um lastro probatório levado pelas partes a um juiz sem poderes instrutórios é um dos principais pontos do processo penal. E como garantir que o vestígio deixado pelo suposto autor do crime será a mesma evidência analisada pelo magistrado? Essa resposta pode ser encontrada na cadeia de custódia (DIAS FILHO, 2012).

A cadeia de custódia, no Brasil, não era regulamentada[6] até a alteração legislativa da Lei 13.964/2019, popularmente conhecida como "Pacote Anticrime" (BRASIL, 2019). Atualmente, ela consta nos artigos 158-A ao 159-F do Código de Processo Penal. Os artigos traçam o procedimento que deve ser seguido, com início na definição de cadeia de custódia:

> 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

[6] Regulamentada, aqui, de forma específica. A cadeia de custódia da prova física já se guiava pelo conteúdo procedimental da Portaria nº 82 de 2014 da Secretaria Nacional de Segurança Pública do Ministério da Justiça. O próprio código de processo penal já continha disposições sobre o assunto (artigo 6º, por exemplo).

> vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. (artigo 158-A, *caput*).

Conforme Geraldo Prado (2014, p. 86), a cadeia de custódia é o "[...] dispositivo dirigido a assegurar a fiabilidade do elemento probatório, ao colocá-lo sob proteção de interferências capazes de falsificar o resultado da atividade probatória.". Badaró (2018, p. 523) a define no mesmo sentido como: "[...] um procedimento de documentação ininterrupta, desde o encontro da fonte de prova, até sua juntada no processo [...]".

E qual a finalidade de manter um procedimento que faça um registro cronológico do vestígio coletado até sua análise pelo Tribunal? A resposta pode ser encontrada em duas palavras: identidade e autenticidade. Identidade, no que diz respeito ao vestígio recolhido na cena do crime e, em como deve ser o mesmo a chegar à mesa do magistrado no momento do julgamento. Integridade, por sua vez, se relaciona ao fato de que a análise feita pelo perito deve seguir o procedimento técnico-científico correto, de forma que, a informação extraída do vestígio e submetida ao contraditório seja íntegra (VALENTE, 2020).

Os aspectos associados a prova digital, como bem elencados acima, tornam a devida execução da cadeia de custódia das provas mais delicado, isso porque, o ambiente digital em que se encontram pode ser alterado sem deixar vestígios óbvios, além de poderem ser acessados ou manuseados à distância, mesmo após sua coleta pelas autoridades periciais (FREITAS, *et al*., 2023, p. 10).

A interrupção da cadeia de custódia é apta a inviabilizar a admissibilidade de uma evidência e as características intrínsecas à prova digital acabam trazendo riscos de manipulação muito altos. Prado expressa muito bem a importância da cadeia de custódia nas provas digitais quando menciona que ela é: "[...] uma garantia de natureza constitucional e não mera consequência lógica do sistema de preservação do corpo de delito digital" (PRADO, 2021, p. 10).

Nesse mesmo sentido, Freitas e Santin trazem a importância da Ciência Forense no âmbito digital e como ela começa antes mesmo do início da cadeia de custódia, estando presente nos procedimentos que envolvem a aquisição até a análise do material, com a preparo de laudo pericial (FREITAS; SANTIN, 2015).

Significa trazer então que a cadeia de custódia deve abranger desde a etapa de recolhimento até o trânsito em julgado do processo. O procedimento relativo ao manuseio das etapas da cadeia de custódia de provas digitais é de caráter fundamental, sendo importante não apenas preservar seu conteúdo, mas o método de recolhimento que elas recebem. Mendes (2020) apresenta que existem 02 (dois) requisitos fundamentais para que uma investigação informática prossiga, são eles: (i) confiabilidade do método de tratamento dos dados e (ii) verificabilidade da idoneidade do método, e que tais resultados podem ser alcançados através de um protocolo procedimental metodologicamente

guiado.

A cadeia de custódia é mais que um mero dispositivo probatório, eis que, conta com medidas que garantem sua fiabilidade e evitam o contágio das crenças do juiz na fundamentação de suas decisões. As provas digitais, entretanto, necessitam de procedimentos específicos, visto suas características intrínsecas. A lei Anticrime trouxe inovações, mas não incluiu em seu texto provas que não sejam físicas e, é muito difícil utilizar uma analogia a essas espécies probatórias, por suas diferenças intrínsecas.

Como visto ao conceituar prova digital, a área forense possui regras importantes no que diz respeito à integridade dos sistemas informáticos e vestígios digitais, as normas ISO/IEC, além de possuir o conceito de vestígio digital e suas características, trazem também um conjunto de procedimentos destinados a garantir a segurança da informação. A preservação desses vestígios vai depender de uma correta coleta, armazenamento, registro, acondicionamento e transporte, paralelamente, relacionados ao aspecto cronológico da cadeia de custódia.

Feito esse breve adendo sobre a área de computação forense porque sua conexão com o direito não deve ser meramente observatório, é preciso que, de fato, seja possível utilizar conceitos desenvolvidos pela área tecnológica, para que seja possível acompanhar as mudanças profundas no sistema legal. Para isso, uma possível aplicação de tecnologia nesse meio seria a conexão da cadeia de custódia com a tecnologia *Blockchain*, como se verá nos capítulos finais do artigo.

CADEIA DE CUSTÓDIA POR MEIO DA TECNOLOGIA *BLOCKCHAIN*

Entendidos os conceitos relativos às características da prova digital e à cadeia de custódia, passa-se a analisar sua aplicação por meio da tecnologia *Blockchain*. Antes disso, faz-se necessário uma breve explicação sobre a tecnologia em si.

APONTAMENTOS INTRODUTÓRIOS SOBRE A TECNOLOGIA *BLOCKCHAIN*

A tecnologia *Blockchain* tem seu início associado à criptomoeda Bitcoin, cuja criação foi anunciada em 2008, em um artigo intitulado: "Bitcoin: *A Peer-to-Peer Electronic Cash System*", publicado por um autor ou grupo de autores sob o pseudônimo de Satoshi Nakamoto (FILIPPI; WRIGHT, 2018). No artigo, Nakamoto apresenta o conceito de *Blockchain* como a tecnologia subjacente ao Bitcoin. A ideia que fundamenta a tecnologia *Blockchain*, proposta por Nakamoto é a de um livro razão que funciona em uma rede de computadores distribuída e usa criptografia para garantir a integridade e imutabilidade dos dados registrados. As transações são agrupadas em blocos, que são adicionados às cadeias após serem verificados por um mecanismo de consenso.

O modelo de confiança da tecnologia *Blockchain* é baseado em um modelo distribuído;

chamado de *trustless trust*, uma "confiança sem confiança" (tradução literal). É como um grande "livro caixa" que armazena pedaços de informações interligados entre si, informações essas armazenadas de forma distribuída. Toda a rede "concorda" com aquela informação, gerando um consenso sobre ela, tornando-a imutável, quase impossível de ser adulterada (DE FILIPPI; WRIGHT, 2018, p. 42)[7].

A tecnologia *Blockchain* nada mais é do que, a formalização para uma estrutura descentralizada que funciona como um "livro razão", que faz registro de todas as transações e suas informações (data, local etc.). As informações, por sua vez, são armazenadas em blocos e a cada período de tempo, é formado um novo bloco de transações, que se liga ao anterior. Esses blocos tornam-se interdependentes e formam uma cadeia (por isso, o nome *block* e *chain*). Sobre sua característica descentralizada, a tecnologia *Blockchain* não armazena suas informações em uma máquina central, nem depende de intermediadores[8].

Cada computador conectado a rede terá uma cópia do "livro razão", tornando as informações seguras. Sua segurança e confiabilidade derivam da descentralização, como cada computador da rede possui um registro das informações, para modificá-los seria quase impossível. Violar uma *Blockchain* é muito difícil. Além das características já citadas, é muito difícil desfazer uma transação realizada por meio da tecnologia *Blockchain*, uma vez que, a informação que é armazenada nos blocos se tornará imutável. Essa imutabilidade garante a integridade dos dados – a *blockchain* consegue garantir o histórico de transações armazenados – e, ao gerar um histórico completo, melhora sua auditoria.

Quanto a operacionalização do consenso em uma *Blockchain*:,a chave para o funcionamento de uma aplicação é que os elementos da rede devem concordar coletivamente sobre o conteúdo adicionado nos blocos. Isso exige um consenso em torno das informações registradas, para que essas se tornem confiáveis. No contexto de uma aplicação baseada em tecnologia *Blockchain*, um *node* (nó) é um computador ou dispositivo que participa da rede. Os *nodes* desempenham um papel fundamental na manutenção da rede, executando várias funções: "Cada *node* dessa rede distribuída age como se fosse um "administrador" do sistema, mantendo uma cópia integral e atualizada de todo o histórico das operações realizadas e registradas na *Blockchain* [...]" (GARCIA, 2021, p. 330).

Em relatório publicado pelo Instituto de Tecnologia e Sociedade do Rio (2018) são analisados os benefícios e desafios da tecnologia. Os principais benefícios estão atrelados à promoção de transparência, segurança e *accountability* e, consequentemente, na redução de fraudes e corrupção. Tais benefícios derivam de características inerentes a tecnologia, resumidamente, são eles: a)

[7] No original, em inglês: *"Because data recorded on a blockchain is visible to all and is hard to repudiate and retroactively modify, groups of people who do not know – and therefore do not trust – one another can rely on this new data structure to coordinate their activity, with less of a need for trusted authorities."*

[8] O mais próximo seriam os mineradores, que verificam e registram informações nos blocos, esses, por sua vez, só poderão adicionar a transação no bloco se a rede concordar, por maioria simples, que a transação é legítima.

temporalidade, ou seja, o fato de cada transação ser codificada e "carimbada" com data e hora, permitindo o rastreamento de todos os blocos da corrente, além de garantir que as transações não sejam alteradas; b) confiança, derivado de seu mecanismo de consenso e recorrente atualização, se trata de um algoritmo que garante que os dados de uma rede sejam os mesmos para todos os participantes; c) resiliência da rede, no caso da Bitcoin *Blockchain*, por exemplo, não há nenhuma ocorrência de queda total na rede ou de ataques que, de fato, tenham comprometido seu funcionamento; d) descentralização, permitindo que a tecnologia opere mesmo em situações extremas como, hipoteticamente, uma grande região que fique sem acesso à internet.

Ao mesmo tempo que essas características explicam o poder da ferramenta para facilitar atividades econômicas e sociais, são elas que representam suas maiores limitações (FILIPPI; WRIGHT, 2018). A natureza sem intermediação e transnacional da *Blockchain* torna a tecnologia difícil de governar e legislar. Como uma aplicação baseada na tecnologia *Blockchain* é pseudônima e têm uma estrutura de dados resistente à manipulação suportada por mecanismos de consenso descentralizados, elas podem ser usadas para coordenar condutas socialmente inaceitáveis ou criminosas. Além disso, por serem transparentes e rastreáveis, qualquer aplicação baseada na tecnologia *Blockchain* está propensa a ser cooptada por governos ou corporações, transformando a tecnologia em uma poderosa ferramenta para vigilância e controle.

Ao descentralizar entidades baseadas em poucos entes certificadores confiáveis, cria-se um paradigma onde existe confiança no sistema em si e, não mais em uma instituição ou agente. Com soluções que tenham por base a tecnologia *Blockchain*, diminui-se a atividade humana, aumentando (até certo ponto) a confiabilidade nas informações, diminuindo-se a subjetividade humana envolvida no processo e, consequentemente, aumentando a agilidade e eficiência de registros. E é exatamente nesse ponto que se conecta os procedimentos de cadeia de custódia, afinal, uma tecnologia que tem como características sua confiabilidade, transparência e, mais importante para o caso, rastreabilidade, é de interesse para que se garanta que não haja a quebra da cadeia de custódia.

A RELAÇÃO ENTRE CADEIA DE CUSTÓDIA E SUA IMPLEMENTAÇÃO POR MEIO DA TECNOLOGIA *BLOCKCHAIN*

A tecnologia *Blockchain* pode ser utilizada como meio de preservação de provas digitais em conjunto à cadeia de custódia, tendo em conta, sua segurança e autenticidade, caracterizando a tecnologia que mantém os registros seguros, inalteráveis e imutáveis. A vantagem de utilizar soluções implementadas por meio da tecnologia nesse processo é a confiabilidade no armazenamento da prova, isto é, há como garantir que a cadeia de custódia não seja quebrada e que a prova não foi alterada: como a prova armazenada na *Blockchain* é validada por vários que integram a rede e todos os passos são

gravados nela, há uma garantia de que a prova não será manipulada.

O ponto fundamental aqui, é que a tecnologia *Blockchain* oferece uma base ideal para estabelecer uma cadeia de custódia confiável para provas digitais. Devido à natureza descentralizada e imutável da tecnologia, as informações registradas permanecem inalteradas e invioláveis, proporcionando uma trilha de auditoria transparente. A ideia trazida quando se conceituava a cadeia de custódia de que há a necessidade de um protocolo procedimental metodologicamente guiado pode encontrar suas respostas na tecnologia.

Em uma investigação criminal, por exemplo, em que evidências digitais precisam ser apresentadas em um tribunal, o uso de uma solução implementada por meio da tecnologia *Blockchain* para registrar essas evidências, protege a cadeia de custódia contra tentativas de manipulação, garantindo que as informações não possam ser contestadas, trazendo uma segurança para o processo.

Seguindo o procedimento de cadeia de custódia disposto no artigo 158-B do Código de Processo Penal (BRASIL, 1941), pode-se imaginar a seguinte situação hipotética: um investigador, lidando com uma prova digital importante para uma investigação criminal, envolvendo um crime de armazenamento de conteúdo ilícito em um disco rígido (HD). Esse investigador possui acesso ao sistema de *Blockchain* criado para lidar com situações específicas envolvendo provas digitais dentro de sua corporação e possui conhecimento dos cuidados que devem ser tomados a respeito da cadeia de custódia. Deve ser levado em consideração, que toda informação depositada na *Blockchain* é divulgada para os *nodes* que integram a rede e, que cada transação conta com informações de data e hora da transação, além de receber um número sequencial específico, para fins de validação.

Nessa situação, o primeiro passo que o investigador deve tomar é o de reconhecimento (artigo 158-B, I, CPP). Este, compreende o ato de distinguir um elemento como de potencial interesse para a produção da prova pericial, logo, quando o investigador identifica o HD como potencial fonte de evidências digitais, cumpre-se essa etapa. Esse evento é então registrado em uma *Blockchain* específica para a investigação, garantindo um registro imutável desse contato inicial, que posteriormente, poderá ser acessado pelo magistrado que poderá confirmar essas informações.

Após o reconhecimento, deve ser feito o procedimento que evita que o estado daquele HD seja alterado, é a etapa do isolamento (artigo 158-B, II, CPP), aqui o disco rígido é isolado e protegido para evitar qualquer alteração nos dados contidos nele durante a investigação. Esse status de isolamento também pode ser registrado na *Blockchain* para controle de acesso e segurança, demonstrando que os dados se mantiveram íntegros.

Em seguida, o investigador procede com a fixação dos dados, feitas com uma descrição detalhada do vestígio, incluindo informações como nomes, datas de criação/modificação e outras características importantes (artigo 158-B, III, CPP). Essa descrição é registrada na *Blockchain*, com

todas as informações necessárias. Os arquivos são então coletados utilizando técnicas e procedimentos que garantem a preservação dos dados originais, sem que haja alteração nos arquivos contidos no disco rígido (artigo 158-B, IV, CPP).

Os arquivos então, serão criptografados e armazenados na *Blockchain* dedicada à evidência, protegendo-os contra adulterações ou acessos não autorizados. (artigo 158-B, V, CPP). Se os arquivos precisarem ser transferidos para outro local para análise adicional, todas as etapas de transporte são registradas na *Blockchain* para garantir uma trilha de auditoria transparente, rastreando todos os movimentos realizados (artigo 158-B, VI, CPP). Se houve transferência da posse do vestígio, no momento do recebimento dos arquivos para análise forense, todas as informações pertinentes como origem, destino e horário de recebimento, são registradas na *Blockchain*, fornecendo um registro seguro de todas as interações feitas até então com os arquivos (artigo 158-B, VII, CPP).

Durante o processamento dos dados (artigo 158-B, VIII, CPP), que é onde ocorre o exame pericial em si, os arquivos são examinados detalhadamente para extrair informações relevantes para a investigação criminal. Os resultados da análise e os arquivos originais são então armazenados (artigo 158-B, IX, CPP) de forma segura na *Blockchain*, associados a um número de registro único que garante sua rastreabilidade e autenticidade. Por último e, se necessário, será realizado o descarte (artigo 158-B, X, CPP) dos arquivos originais do disco rígido, que é feito de acordo com os procedimentos legais aplicáveis, com um registro seguro na *Blockchain* para documentar todas as etapas da cadeia de custódia.

A tecnologia *Blockchain*, como visto anteriormente, é reconhecida por sua capacidade de fornecer um registro imutável e seguro das transações e informações armazenadas. As evidências armazenadas em uma *Blockchain* desfrutam de um alto nível de segurança devido a natureza da tecnologia, conhecida por sua imutabilidade e resistência a violações. Isto é, por ser uma estrutura descentralizada e distribuída, composta por uma rede de *nodes* interconectados, cada um com uma cópia completa do registro de transações, para violar uma informação armazenada sobre essa evidência, seria necessário alterar o registro em todos os nós da rede simultaneamente, o que é extremamente desafiador e exige um grande poder computacional, beirando o impossível.

Em *Blockchains* públicas[9], como a do Bitcoin, por exemplo, a segurança é reforçada pelo mecanismo chamado *Proof-of-Work* (PoW)[10], que exige uma quantidade massiva de poder computacional para modificar retroativamente transações antigas. Além disso, sua imutabilidade é

[9] A *Blockchain* pública é como uma rede aberta e transparente, acessível a todos, enquanto, a *Blockchain* privada se assemelha a uma rede privativa, controlada por uma entidade específica e utilizada para fins específicos, como gerenciamento interno de dados e transações.
[10] O *Proof-of-Work* é um conceito utilizado em sistemas de *Blockchain*, como o Bitcoin, para validar e garantir a segurança das transações na rede.

garantida pela cadeia de blocos encadeadas de forma criptograficamente segura, onde cada bloco contém um *hash*[11] do bloco anterior. Mesmo em *Blockchains* privadas, onde a governança pode ser mais centralizada, a segurança ainda se mantém por meio de mecanismos de consenso específicos e controles de acesso rigorosos entre os participantes autorizados.

Um modelo que se adequa ao caso é o sugerido por Alruwaili (2021), o *CustodyBlock* (CB). O modelo utiliza um protocolo de *blockchain* privado e contratos inteligentes[12] para apoiar o controle, transferência, análise e monitoramento da preservação de evidências. O algoritmo proposto utiliza a tecnologia *Hyperledger*, uma plataforma de livro-razão de código aberto criada pela *International Business Machines Corporation* (IBM). O *Hyperledger* suporta contratos inteligentes chamados de *chaincodes* (GHOLAMREZA; LEUNG, 2018), programas responsáveis por executar um acordo (consenso) entre membros da rede. Esses *chaincodes* podem aprovar blocos e enviar transações para blocos confiáveis e previamente aprovados, a fim de serem validados e autorizados.

Comentado [A1]: Adição do CustodyBlock (CB)

Alruwaili (2021) teve como objetivo em seu trabalho revisar as dificuldades e formular sugestões para tornar o procedimento da cadeia de custódia de evidências digitais mais confiável e alinhado às necessidades dos tribunais, independentemente do país, da empresa ou da ferramenta por meio da qual as evidências digitais são coletadas, defendendo a utilização da tecnologia *blockchain* para melhorar o processo e o ciclo de vida do manuseio das evidências.

Desta forma, o modelo conceitual proposto tem como intenção preencher lacunas na literatura e enfrentar os desafios relacionados ao manuseio de evidências digitais, visando transformar de forma eficiente a prática jurídica global. O modelo CB demonstra como uma rede *blockchain* e os contratos inteligentes podem oferecer acesso monitorado e rastreável à cadeia de evidências para os participantes envolvidos, como autoridades policiais, tribunais, escritórios de advocacia, entre outros (ALRUWAILI, 2021).

A arquitetura do sistema inclui participantes (autoridades policiais, provedores de serviços em nuvem, validadores)[13], um algoritmo de consenso, contratos inteligentes, funções criptográficas e assinaturas digitais. A autoridade policial é o principal ator do modelo CB, é ela que define os papéis relacionados aos controles de leitura/escrita das transações do CB e do livro-razão. Da mesma forma, é a autoridade policial que estabelece as regras que devem ser escritas/codificadas em contratos inteligentes para automatizar o registro e a integração de entidades. As testemunhas digitais colaboram

[11] O *hash* é como uma impressão digital de cada bloco. Se refere a uma função matemática que transforma dados em uma sequência de caracteres alfanuméricos de comprimento fixo.
[12] Programas ou códigos autoexecutáveis armazenados em uma *blockchain* que automatizam a execução de termos e condições previamente acordados entre as partes. Esses contratos eliminam a necessidade de intermediários, pois são programados para operar de forma autônoma assim que os critérios estabelecidos são atendidos.
[13] Tradução livre dos participantes da arquitetura do sistema, do original: "[...] *law enforcement, cloud service providers, validators* [...]".

fornecendo evidências baseadas em incidentes ou sensores, dentro de suas capacidades, e essas evidências são analisadas também pela autoridade policial (ALRUWAILI, 2021).

O *CustodyBlock* demonstra como a tecnologia *Blockchain* e os contratos inteligentes podem oferecer acesso monitorado e rastreável à cadeia de custódia, além de apresentar uma plataforma onde os dados forenses podem ser armazenados sem risco de ataques, servindo como uma metodologia segura para a preservação e o manuseio de evidências (ALRUWAILI, 2021).

Observado o caso hipotético e o modelo do *CustodyBlock* (CB), é possível atestar como os protocolos executados por uma solução implementada pela tecnologia *Blockchain* exigem procedimentos que asseguram que a informação é verdadeira e que a evidência coletada será aquela efetivamente analisada pelo juiz, que poderá verificar todo o caminho traçado, desde sua coleta até eventual descarte, se necessário. Embora a segurança da *Blockchain* não seja absoluta e possa ser influenciada por fatores como vulnerabilidades na implementação ou ataques específicos, sua arquitetura robusta e mecanismos de segurança incorporados fazem dela uma opção altamente confiável para o armazenamento e verificação de evidências digitais no contexto envolvendo provas digitais e cadeia de custódia.

CONSIDERAÇÕES FINAIS

O artigo se desenvolveu no contexto da sociedade informacional e da necessidade de tutela adequada de provas digitais e se guiou a partir da seguinte pergunta de pesquisa: a cadeia de custódia da prova digital pode ser efetivada por meio da implementação da tecnologia *Blockchain*?

Diante deste cenário, se buscou explanar acerca da sociedade informacional e como esta modificou as formas de práticas delitivas, o que demonstra seu impacto em matéria probatória no âmbito processual penal. Neste panorama, foi indicada a tecnologia *Blockchain,* como meio de preservação da cadeia de custódia das provas digitais, vez que, respeita as disposições normativas e eleva a segurança processual ao conferir um registro transparente e imutável do caminho pelo qual aquela evidência, discutida no processo penal, percorreu. Logo, se confirmou a hipótese de que a tecnologia *Blockchain* se mostra como uma alternativa viável para a cadeia de custódia das provas digitais.

Entre as soluções apresentadas, destacou-se o modelo *CustodyBlock* (CB), conforme sugerido por Alruwaili (2021). Esse modelo utiliza a tecnologia *Hyperledger*, um protocolo de *blockchain* privado que permite a execução de contratos inteligentes (*chaincodes*) para automatizar o controle, a transferência, a análise e o monitoramento das evidências digitais. A arquitetura do sistema inclui participantes como autoridades policiais, provedores de serviços em nuvem e validadores, além de algoritmos de consenso e assinaturas digitais, todos voltados para garantir a integridade da cadeia de

custódia.

Em resumo, o que se observa é que a aplicação da tecnologia *Blockchain* em um sistema que ainda está se adaptando à era digital, pode representar uma mudança transformadora, oferecendo maior transparência, segurança e eficiência na gestão das provas digitais. No entanto, é crucial abordar cuidadosamente os desafios e considerações legais para garantir uma integração harmoniosa e eficaz dessa tecnologia inovadora no contexto jurídico.

REFERÊNCIAS

ALRUWAILI, Fahad F. **CustodyBlock: A Distributed Chain of Custody Evidence Framework**. Information, 2021. 12(2):88. Disponível em: https://doi.org/10.3390/info12020088 Acesso em: 02 dez. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO/IEC 27037:2013: **Tecnologia da informação - Técnicas de segurança - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.** Rio de Janeiro: ABNT, 2013.

BADARÓ, Gustavo Henrique. **A cadeia de custódia e sua relevância para a prova penal.** *In*: SIDI, Ricardo; LOPES, Anderson Bezerra (orgs.). Temas atuais da investigação preliminar no processo penal. 1. reimp. Belo Horizonte: Editora D'Plácido, 2018

BADARÓ, Gustavo. **Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia**. Boletim IBCCRIM, ano 29, n. 343, p. 7-9, jun. 2021. Disponível em: https://ibccrim.org.br/publicacoes/edicoes/747/8544. Acesso em: 02 dez. 2024.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação.** Rio de Janeiro: Lumen Juris, 2018.

BRASIL. **Decreto n. 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001. Acesso em: 02 dez. 2024.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal.. Brasília, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 02 dez. 2024.

BRASIL. **Lei nº 3.689, de 03 de outubro de 1941**. Código de Processo Penal. Brasília, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm Acesso em: 02 dez. 2024.

BRETAS, Adriano. **Apontamentos de Processo Penal**. Curitiba: Sala de Aula Criminal, 2017.

CASEY, Eoghan. **Digital evidence and computer crime: forensic, science, computer and the internet.** 2 ed. San Diego/London: Enselvier Academic Press, 2004.

CASTELLS, Manuel. **A sociedade em rede.** 8. ed. rev. e ampl. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, 2005.

DIAS FILHO, Claudemir Rodrigues. **Cadeia de custódia: do local de crime ao trânsito em julgado; do vestígio à evidência.** Revista Brasileira de Ciências Criminais, v. 3, p. 393-408, 2012.

FILIPPI, Primavera de; WRIGHT, Aaron. **Blockchain and The Law: The Rule of Code.** 3. ed. Cambridge, Massachusetts: Harvard University Press, 2018.

FREITAS, Cinthia Obladen de Almendra; SANTIN, Altair Olivo. Forense Computacional. In: GARRIDO, Rodrigo Grazinoli; GIOVANELLI, Alexandre (org.). **Ciência Forense: uma introdução à criminalística.** 2. ed. Rio de Janeiro: Projeto Cultural, 2015. p. 195-199.

FREITAS, Cinthia Obladen de Almendra; SILVA, Rui Miguel; SOUSA, Devilson da Rocha; PIRATELLI, João Paulo Machado. **A cadeia de custódia de provas digitais sob a perspectiva da forense digital: considerações a partir de uma perspectiva tecno-científica.** Revista Síntese de Direito Penal e Processual Penal, Brasília, v. 23, n. 141, p. 101-123, ago./set., 2023.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. **Apontamentos sobre a Cadeia de Custódia da Prova Digital no Brasil.** Revista em Tempo, Marília, v. 20, n. 1, nov. 2020. https://doi.org/10.26729/et.v20i1.3130. Acesso em: 02 dez. 2024.

GARCIA, Flúvio Cardinelle Oliveira. **Corrupção econômica, Accountability Sociodigital e Blockchain: uma proposta para enfrentamento do fenômeno corruptivo por meio do rastreamento de verbas públicas no marco da revolução digital.** Rio de Janeiro: Lumen Juris, 2021.

HAN, Byung Chul. **Infocracia: Digitalização e a crise da democracia**. Tradução de Gabriel S. Philipson. Petrópolis: Vozes, 2022.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Blockchain para aplicações de interesse público.** Rio de Janeiro, 2018. Disponível em: https://itsrio.org/wp-content/uploads/2019/03/Relatório-ITS-GE-Blockchain-vFinal.pdf. Acesso em: 02 dez. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000:2018. **Information technology Security techniques Information security management systems**. 5. ed. 2018.

KHALED JÚNIOR, Salah H. **A Busca da Verdade no Processo Penal: para além da ambição inquisitorial.** 2. ed. Belo Horizonte: Casa do Direito, 2016.

KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019.

LOPES JUNIOR, Aury. **Direito Processual Penal**. 16. ed. São Paulo: Saraiva Educação, 2019.

MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal: entre a proteção de dados e a infiltração por software.** Salvador: Juspodivim, 2020.

OLIVEIRA, Vinicius Machado de. **ABNT NBR ISO/IEC 27037:2013**. Academia de Forense Digital. São Paulo, 2018. Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/. Acesso em: 02 dez. 2024.

PIRATELLI, João Paulo Machado; FREITAS, Cinthia Obladen de Almendra. **Persecução Penal e Provas Digitais obtidas a partir de Dispositivos Móveis: entre a coleta e a preservação da prova e a ilicitude probatória.** In: ENCONTRO INTERNACIONAL DO CONPEDI. 11. Direito, Governança e Novas Tecnologias. Santiago, Chile. Anais [...]. Santiago, Chile, 2022. p. 159-178. Disponível em: http://site.conpedi.org.br/publicacoes/129by0v5/4yglxo10/378eRIbv715pBw0l.pdf. Acesso em: 02 dez. 2024.

PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital.** [S.l.]: [s.d.], 2021. Disponível em: https://www.conjur.com.br/dl/ar/artigo-geraldo-prado.pdf. Acesso em: 02 dez. 2024.

PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por meios ocultos**. 1. ed. São Paulo: Marcial Pons, 2014.

RAMEZAN, Gholamreza; LEUNG, Cyril. **A blockchain-based contractual routing protocol for the internet of things using smart contracts**. Wirel. Commun. Mob. Comput. 2018. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1155/2018/4029591 Acesso em: 02 dez. 2024.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. 1. ed. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.

VALENTE, Manuel Monteiro Guedes. **Cadeia de Custódia da prova**. 2. ed. Coimbra: Edições Almendina, 2020.

VAZ, Denise Piovani. **Provas Digitais no Processo Penal: formulação de conceito, definição de características e sistematização do procedimento probatório**. 198fls. 2012. Tese (Doutorado). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php. Acesso em: 02 dez. 2024.