XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO II

THIAGO ALLISSON CARDOSO DE JESUS

DANI RUDNICKI

LUIZ BRÁULIO FARIAS BENÍTEZ

Copyright © 2022 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU – São Paulo
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR – Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade – UNIMAR/FEPODI – São Paulo

Conselho Fiscal:
Prof. Dr. Caio Augusto Souza Lara – ESDHC – Minas Gerais
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. José Filomeno de Moraes Filho – Ceará
Prof. Dr. Lucas Gonçalves da Silva – UFS – Sergipe
Prof. Dr. Valter Moura do Carmo – UNIMAR – São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Daniela Marques De Moraes – UNB – Distrito Federal
Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM – São Paulo
Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie – São Paulo
Comunicação:
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul
Profa. Dra. Maria Creusa De Araújo Borges - UFPB – Paraíba
Prof. Dr. Matheus Felipe de Castro - UNOESC – Santa Catarina
Relações Internacionais para o Continente Americano:
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM – Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
Relações Internacionais para os demais Continentes:
Prof. Dr. José Barroso Filho – ENAJUM
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
Eventos:
Prof. Dr. Antônio Carlos Diniz Murta - Fumec – Minas Gerais
Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC – Paraná
Profa. Dra. Livia Gaigher Bosio Campello - UFMS – Mato Grosso do Sul

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UMICAP – Pernambuco

D597

Direito penal, processo penal e constituição II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Dani Rudnicki; Luiz Bráulio Farias Benítez; Thiago Allisson Cardoso De Jesus.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-639-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal e constituição.

XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO II

Apresentação

APRESENTAÇÃO

Ambiência de riscos e intensas rupturas com os marcos constitucionais e convencionais, a contemporaneidade brasileira afigura-se na efervescência de diversos paradigmas e teorias, influências para as políticas criminais que são (re)dimensionadas a partir de interesses e racionalidades, alguns declarados e outros implícitos, que se desdobram na forma como o Estado, estrutura-estruturante, lida com os problemas penais, compatibilizando-se ou não com os preceitos de base garantista-humanitária.

Nessa senda, afigura-se a presente obra coletiva como instrumento fecundo para publicização de pesquisas científicas, reunindo os artigos submetidos e aprovados ao Grupo de Trabalho Direito Penal, Processo Penal e Constituição II para apresentação no XXIX Congresso Nacional do Conselho Nacional de Pesquisa e Pós-Graduação em Direito/CONPEDI, realizado no período de 07 a 09 de dezembro de 2022, na linda Balneário Camboriú/SC com esmero organizado a partir da cooperação interinstitucional de grandes IES e sediado na Universidade do Vale do Itajaí/Univali, campus de excelência internacional.

Na pauta, a compatibilidade do processo penal com os marcos constitucionais e com a perspectiva dos direitos humanos; bem como a sistematização de dados sobre pesquisas acadêmicas sobre encarceramento feminino no Brasil, olhando para o Sul e projetando discussões para o país e para o mundo. No compasso das urgentes discussões, a expansão do Direito Penal, a construção do inimigo e as estratégias de aniquilamento, do uso da dor e da estigmatização dos que estão em conflito com a lei penal; no viés do gênero, a análise do instituto da prisão preventiva em sede de encarceramento feminino no âmbito de um Tribunal de Justiça, retratando regionalmente um problema enfrentado nacionalmente, inovando na crítica e nas reflexões silenciadas e as análises em torno da Lei de Stalking como estratégia na proteção de mulheres em situação de violência.

Na construção das verdades, percepção de riscos e reflexões sobre o sistema de responsabilização penal do ente coletivo e as repercussões do pânico moral em contexto de processo penal midiático, espetacularizado e violador de direitos. Na toada da inovação e das novas pautas para o Sistema de Justiça Criminal, os fundamentos da seletividade dos

criminalizados no enfrentamento da questão da drogadição pelo sistema Penal; a investigação defensiva e as repercussões para a ampla defesa; e o uso da videoconferência para a realização da audiência de custódia sob a ótica dos atores envolvidos na procedimentalização. Ademais, contributos sobre as nuances da teoria do Bem Jurídico-Penal à partir da prestabilidade como categoria analítica na obra de Zaffaroni; notas sobre a implementação de acordo de não-persecução penal no âmbito da polícia civil brasileira; a configuração do engano qualificado no estelionato; e o reconhecimento da criminalidade na sua expressão global e suas emergências de cooperação internacional e uso de medidas extrapenais para contenção e enfrentamento.

Reunindo pesquisadores/as por excelência, vinculados às diversas Instituições de Ensino Superior - públicas e privadas, nacionais e estrangeiras; a presente obra que ora apresentamos demonstra a qualidade da pesquisa jurídica no Brasil no campo criminal bem como a audácia, o rigor científico e a vivacidade de autores/as em enfrentar temas necessárias para compreender, reflexivamente, os tempos atuais e desenvolver capacidades propositivas. De fato, pesquisar exige cuidados, sobretudo quando a pesquisa chega ao seu ápice! É nesse momento, então, que precisamos deixá-la ir, sem apegos e sem vaidades, inserindo-a no mundo concreto, real, carente de discussões, no qual a Academia, por meio de lutas e resistências, cumprirá o seu desiderato!

Viva o pensamento crítico e a produção de conhecimento engajado e inteligente de nosso país! Zelemos para que esse espaço seja sempre assim!

Prof. Dr. Dani Rudnicki

Universidade La Salle

danirud@hotmail.com

Prof. Dr. Luiz Bráulio Farias Benitez

Universidade do Vale do Itajaí

lbfbenitez@hotmail.com

Prof. Dr. Thiago Allisson Cardoso de Jesus

Universidade Estadual do Maranhão, Universidade Ceuma/Mestrado em Direito e Afirmação de Vulneráveis e Programa de Doctorado en Estado de Derecho y Gobernanza Global/USAL-ES

t_allisson@hotmail.com

A CRIPTOGRAFIA COMO MECANISMO DE PROTEÇÃO DE PROVAS DIGITAIS NA CADEIA DE CUSTÓDIA

CRYPTOGRAPHY AS A MECHANISM TO PROTECT DIGITAL EVIDENCE IN THE CHAIN OF CUSTODY

Cinthia Obladen de Almendra Freitas [1]
João Paulo Machado Piratelli [2]
Devilson Da Rocha Sousa

Resumo

A prova se apresenta como um dos principais elementos processuais do direito penal, por isso a garantia de sua integridade, autenticidade e inviolabilidade são fundamentais para a observância do devido processo legal e garantia do direito à ampla defesa. A Lei Nº 13.964 /2019 veio instituir a Cadeia de Custódia, estabelecendo a forma para coleta, armazenamento e preservação cronológica dos vestígios probatórios. Porém, a lei não faz menção a esses procedimentos no que se refere às provas digitais. Busca-se contribuir com aspectos jurídicos e tecnológicos para Cadeia de Custódia no meio digital. Questiona-se: A criptografia pode ser utilizada para conferir maior proteção às provas digitais no contexto da cadeia de custódia? Fez-se uso do método de pesquisa hipotético-dedutivo, apoiando-se em técnicas de pesquisa bibliográfica e legislativa. Evidencia-se que, apesar de o Superior Tribunal de Justiça ter declarado que a inviolabilidade da cadeia de custódia não gera de imediato a nulidade da prova em questão, a manutenção da integridade e a garantia de sua inviolabilidade são medidas que se impõe no meio digital, sendo a criptografia dos elementos probatórios coletados necessária tanto no âmbito jurídico quanto no tecnológico.

Palavras-chave: Processo penal, Cadeia de custódia, Provas digitais, Criptografia, Superior tribunal de justiça

Abstract/Resumen/Résumé

The evidence presents itself as one of the main procedural elements of Criminal Law, so the guarantee of its integrity, authenticity and inviolability are fundamental for the observance of due process of law and guarantee of the right to ample defense. Act 13,964/2019 instituted the Chain of Custody, establishing the way for the collection, storage and chronological preservation of evidentiary traces. However, this Act makes no mention of these procedures with regard to digital evidence. It seeks to contribute with legal and technological aspects to the Chain of Custody in the digital means. The question is: Can cryptography be used to

[1] Doutora em Informática Aplicada. Coordenadora do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná – PUCPR.

[2] Mestrando pelo Programa de Pós-Graduação em Direito (PPGD) da Pontifícia Universidade Católica do Paraná – PUCPR.

provide greater protection to digital evidence in the context of the chain of custody? The hypothetical-deductive research method was applied to, supported by bibliographic and legislative research techniques. It is evident that, despite the Superior Court of Justice having declared that the inviolability of the chain of custody does not immediately generate the nullity of the evidence in question, the maintenance of integrity and the guarantee of its inviolability are measures that are imposed in the digital means, with the encryption of the collected evidence being necessary both in the legal and technological aspects.

Keywords/Palabras-claves/Mots-clés: Criminal proceedings, Chain of custody, Digital evidences, Cryptography, Superior court of justice

1. INTRODUÇÃO

No Direito Penal, assim como em todas as outras áreas do Direito, o instituto da prova se apresenta como um dos principais, se não o principal, elementos processuais, sendo fundamental para a discussão do tema e das questões que são trazidas à apreciação pelo Poder Judiciário, uma vez que o estudo e reflexos do processo judicial passam pela discussão da materialidade e da constatação da existência de determinada conduta antijurídica, ilícita.

Nesse sentido, a garantia da integridade, autenticidade e inviolabilidade dos elementos probatórios são fundamentais para a existência do processo judicial e, mais que isso, para a observância do devido processo legal e garantia do direito à ampla defesa. Tamanha a sua importância, a Constituição Federal reservou atenção especial em um de seus dispositivos, mais precisamente no o art. 5º, inciso LVI, sendo inadmissíveis, no processo, as provas obtidas por meios ilícitos.

Contudo, não basta que no processo a prova exista e seja suficientemente capaz de indicar a autoria de determinado ato antijurídico, é, também, imprescindível que sua integridade, autenticidade e inviolabilidade, bem como o devido manuseio sejam também garantidos e comprovados. Foi por conta desse cenário e de sua importância, bem como, intentado instituir em nível nacional um procedimento que fosse capaz e suficiente para estabelecer a forma como tal elemento deveria ser colhido, preservado e armazenado, que a Lei nº 13.964, de 24 de dezembro de 2019, instituiu a cadeia de custódia no Processo Penal.

A citada Lei representou um avanço significativo no que se refere a preservação e devida manipulação da prova processual no âmbito penal, não sendo possível hoje dissociar uma da outra. Apesar dessa evolução louvável, o legislador perdeu uma ótima oportunidade para também instrumentalizar o procedimento da cadeia de custódia em meio digital, ou mesmo, estabelecer as eventuais diferenças ou distinções que devem ser observadas quando da execução desse procedimento no mundo físico e no mundo digital.

Diante desse cenário e considerando a importância do tema para a sociedade e para o Direito, em especial para o Direito Penal, e apesar de decisão do Superior Tribunal de Justiça ter declarado que a inviolabilidade da cadeia de custódia não gera de imediato a nulidade da prova em questão, o estudo ora realizado discute aspectos tecnológicos da aplicação da criptografia para a garantia da integridade de provas digitais. A decisão do STF aponta que eventuais irregularidades devem ser observadas pelo juízo ao lado dos demais elementos produzidos durante a instrução criminal para, então, decidir se a prova questionada pode ser considerada confiável. Só após essa confrontação é que o magistrado, caso não encontre

sustentação na prova cuja cadeia de custódia foi violada, pode retirá-la dos Autos ou declará-la nula.

O artigo segue apresentando os aspectos e as nuances da cadeia de custódia no contexto brasileiro, para se debruçar sobre a aplicação da criptografia na cadeia de custódia de provas digitais e, então, apontar os reflexos e as vantagens do uso da criptografia nesse contexto. O artigo é resultado de projeto de pesquisa financiado pelo Programa de Cooperação Acadêmica em Segurança Pública e Ciências Forenses (PROCAD/SPCF) da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

2. A CADEIA DE CUSTÓDIA NO CONTEXTO BRASILEIRO E A PROVA DIGITAL

Em 23 de janeiro de 2020, entrou em vigor a Lei nº 13.964, de 24 de dezembro de 2019, apelidada de "Pacote Anticrime" (BRASIL, 2019), buscando-se aperfeiçoar o Sistema de Justiça Criminal para torná-lo mais célere e eficiente, diminuindo, assim, a criminalidade como um todo. E, como o escopo desse artigo é o instituto da cadeia de custódia, tem-se o Pacote Anticrime como cenário brasileiro, de modo a relacionar as normas processuais com as provas digitais de interesse processual-penal.

Para a doutrina, a cadeia de custódia é um "mecanismo garantidor da autenticidade das evidências coletadas e examinadas, assegurando que correspondem ao caso investigado, sem que haja lugar para qualquer tipo de adulteração" (LIMA, 2020, p. 718). Em outras palavras, a "cadeia de custódia exige o estabelecimento de um procedimento regrado e formalizado, documentando toda a cronologia existencial daquela prova, para permitir a posterior validação em juízo e exercício do controle epistêmico" (LOPES JÚNIOR, 2022, p. 1036). Entende-se tal qual Prado (2014) que a cadeia de custódia configura conjunto de métodos pelos quais se pretende assegurar, a partir de um sequenciamento cronológico, a preservação, a integridade, a autenticidade e a invulnerabilidade do conjunto probatório.

E foi no mesmo sentido desses entendimentos que o legislador conceitua, no art. 158-A, cadeia de custódia como "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" (BRASIL, 2019).

E além de definir o conceito, o Pacote Anticrime passou a regulamentar expressamente a cadeia de custódia ao discipliná-la por meio da inserção dos artigos 158-A a 158-F no Código de Processo Penal (CPP). As mudanças trazidas por essa alteração legislativa representam um

avanço no estudo da temática da cadeia de provas no Brasil, contudo, esse avanço deve ser visto com certa ressalva, em especial, por 02 (dois) fatores, a saber:

1) ausência de um ou mais dispositivos legais que busquem abordar a instauração e execução da cadeia de custódia no ambiente digital, fator esse que traz significativos prejuízos à boa execução da cadeia de custódia nesse ambiente na medida em que o meio digital está sujeito a variáveis e intercorrências diferentes do mundo físico. Um bom exemplo disso pode ser percebido no fato de que, no ambiente digital, a noção de tempo e espaço se alteraram e se expandem para além do que se compreende no mundo físico, fatores esses que alteraram significativamente a forma de condução das etapas da cadeia de custódia;
2) ausência de inovação do legislador no que se refere às melhorias já trazidas pela Portaria SENASP nº 82, de 16 de julho de 2014 do Ministério da Justiça, a qual já estabelecia as diretrizes sobre os procedimentos a serem observados, por todos os órgãos da Justiça, no tocante à cadeia de custódia de vestígios. Essa Portaria serviu durante muitos anos como guia mestre no que se refere à correta coleta, armazenamento e manuseio de prova processual.

E foi essa Portaria, juntamente com o posicionamento doutrinário formado no Brasil que possibilitou que o Superior Tribunal de Justiça (STJ), ainda em 2014, consolidasse o entendimento acerca da aplicabilidade e emprego da cadeia de provas no Brasil quando da análise e julgamento do *Habeas Corpus* nº 160.662/RJ (SUPERIOR TRIBUNAL DE JUSTIÇA, 2014).

Cabe aqui um questionamento relevante ao estudo desenvolvido, visto que pelos vocábulos utilizados pelo legislador no momento da redação dos artigos 158-A a 158-F, poder-se-ia alegar que o procedimento da cadeia de custódia não se aplicaria à provas digitais devido à ausência de uma concretude palpável, como ocorre, por exemplo, com um cadáver no crime de homicídio ou com a substância ou droga de abuso apreendida em um cenário de crime de tráfico. Mas não estaria a prova digital inserida no conjunto probatório, independentemente do meio em que se encontra ou de coleta? Esse questionamento auxiliou os estudos ora realizados.

No julgado do *Habeas Corpus* nº 160.662/RJ, a Ministra Assusete Magalhães ao tratar da cadeia de custódia em operação da Polícia Federal, firmou entendimento de que o material probatório produzido no decorrer de uma interceptação não deveria servir unicamente "aos interesses do órgão acusador, sendo imprescindível a preservação da sua integralidade, sem a qual se mostra inviabilizado o exercício da ampla defesa, tendo em vista a impossibilidade da

efetiva refutação da tese acusatória, dada a perda da unidade da prova" (SUPERIOR TRIBUNAL DE JUSTIÇA, 2014, p. 13).

Seguindo o raciocínio, a Ministra da Corte Superior considerou como "lesiva ao direito à prova, corolário da ampla defesa e do contraditório – constitucionalmente garantidos –, a ausência da salvaguarda da integridade do material colhido na investigação, repercutindo no próprio dever de garantia da paridade de armas das partes adversas" (SUPERIOR TRIBUNAL DE JUSTIÇA, 2014, p. 13). Ou seja, sem que fosse possível a todas as partes do processo criminal ter acesso à íntegra da prova, não seria possível utilizá-la em juízo, visto restar prejudicada a sua análise global, seja do ponto de vista da rastreabilidade, seja da própria integridade e autenticidade do que consta no processo.

Desse modo, pode-se identificar que cadeia de custódia guarda íntima relação com a garantia da legalidade e licitude da prova processual na medida em que o art. 5º, inciso LVI, da Constituição Federal vem positivar o direito fundamental à prova ao dispor que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos" (BRASIL, 1988). Sendo importante destacar que no corolário da ilicitude também está, ou deveria estar, a garantia de sua inviolabilidade e integridade, na medida em que a licitude não garantida unicamente no momento da coleta da prova, mas também, e especialmente, durante o seu armazenamento, processamento, análise e descarte.

Menciona-se, portanto, a Teoria dos Frutos da Árvore Envenenada, em língua inglesa "*fruit of the poisonous tree doctrine*", originada no caso *Silverthorne Lumber Company, Inc., et al. v. United States*, julgado pela Suprema Corte do Estados Unidos, em 1920 (CARVALHO, 2014). Essa teoria é uma maneira didática de explicar as provas ilícitas por derivação, segundo a qual entende-se que se uma prova é obtida ilicitamente, tudo que dela derivar também será ilícito e, portanto, imprestável para o processo, devendo ser desentranhado dos Autos. É nesse contexto que a cadeia de custódia ganha relevância, porque garante a rastreabilidade da prova, o que é imprescindível para análise de eventual ilicitude probatória por derivação.

Em síntese, além das discussões doutrinárias, ao menos desde 2014, o Brasil possuía precedente judicial tratando a integridade da prova como garantia processual das partes do processo. Com a positivação trazida pelo Pacote Anticrime, a aplicação da cadeia de custódia no Processo Penal brasileiro passou, ou melhor, deveria passar, a ser imperativa e indubitável, haja vista a desnecessidade de exercícios hermenêuticos mais elaborados para extraí-la do texto constitucional, o que caso não fosse respeitado, poderia ensejar, em certa medida, arbítrios jurisdicionais e erros judiciários danosos às garantias processuais. Mas é necessário ponderar,

que erros tecnológicos também podem ser danosos às garantias processuais quando as provas decorrem de meio digital.

Apesar disso, recentemente o mesmo Superior Tribunal de Justiça quando do julgamento do *Habeas Corpus* 653515(2021/0083108-7 de 01/02/2022) resolveu inovar ao destacar que eventual violação da cadeia de custódia não implica obrigatoriamente a nulidade ou a inadmissibilidade da prova coletada. Por mais contrassenso que esse posicionamento possa parecer, o que o Superior Tribunal passou a aceitar e defender foi a tese de que eventuais irregularidades na cadeia de custódia devem ser, por parte do juiz, analisadas juntamente com os demais elementos probatórios, inclusive com a dinâmica dos acontecimentos e com a alegações produzidas pelas partes (SUPERIOR TRIBUNAL DE JUSTIÇA 2021).

A argumentação trazida pela corte se baseou no fundamento de que, apesar de o legislador ter trazido nos artigos 158-A a 158-F do CPP de forma detalhada as fases de execução da cadeia de custódia, em especial naquilo que se refere a preservação da prova, também é certo que esse mesmo legislador restou inerte ou em silêncio "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" (SUPERIOR TRIBUNAL DE JUSTIÇA, 2021, p. 2).

Não é forçoso argumentar que com tal posicionamento, há verdadeiro enfraquecimento deste que é um dos principais, se não o principal, instituto do direito processual criminal e também cível, na medida em que se a prova pode estar sujeita a violações ou interferências externas, que garantias teria a parte ré ou o acusado de que determinada prova não foi adulterada para lhe prejudicar ou impingir determinada materialidade? Aqui importa frisar, como inclusive foi destacado no julgado em questão, que a cadeia de custódia não é um mero procedimento jurisdicional que pode ou não ser instituído, muito pelo contrário, o seu emprego e sua observação dizem respeito à garantia da idoneidade do caminho percorrido pela prova até sua análise pelo magistrado e pelas partes, incluindo-se peritos e assistentes técnicos quando cabível, sendo indiscutível que qualquer alteração no seu emprego ou a interferência durante o trâmite processual é passível de gerar a imprestabilidade de todo o material probatório.

Além disso, não há que se mencionar a manutenção do devido processo legal, nem mesmo, os direitos à ampla defesa e a garantia de utilização processual unicamente de provas lícitas, se a cadeia de custódia restou violada ou inobservada, mesmo que havendo possibilidade de amplo acesso às provas objetos de violação ou de sua reanálise por parte de perito, como alegou o Superior Tribunal de Justiça (SUPERIOR TRIBUNAL DE JUSTIÇA, 2021).

Se no que se refere a provas materiais essa discussão já é sensível, quando se observa o cenário das provas digitais tem-se contornos ainda mais complexos, na medida em que, como já destacado, o mundo digital possui uma relação mais complexa com a questão da materialidade e rastreabilidade de elementos probatórios, tendo-se em vista a volatilidade nos meios de armazenamento, o que facilitar adulterações[1], obliterações[2] e ocultações[3], as quais podem ocorrer sem deixar vestígios ou rastros evidentes para não especialistas. Isso torna possível a violação da cadeia de custódia sem a consequente invalidade da prova uma grande desvantagem ao acusado/réu do processo penal, podendo significar a inversão do ônus probatório, na medida em que caberá ao este último agente demonstrar que a prova foi adulterada/obliterada/ocultada e mais, que essa adulteração/obliteração/ocultação pode resultar em prejuízos processuais a ele, quando em verdade deveria ser o órgão acusador o responsável por tal comprovação. Considerando-se o exposto, segue-se com o estudo da aplicação das técnicas de criptografia na cadeia de custódia de provas digitais.

3. A APLICAÇÃO DA CRIPTOGRAFIA NA CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS E SUA IMPORTÂNCIA TÉCNICA

Apesar do recente julgado do Superior Tribunal de Justiça, que terá seus efeitos e limites ainda discutidos futuramente, salvo decisão em contrário, a violação da cadeia de custódia implica a impossibilidade da valoração da prova, fato este que implica no seu exame – no exame de verificação de cumprimento de todos os requisitos inerentes à cadeia de custódia, como elemento fundamental e um dos objetos do juízo de admissibilidade.

Tal premissa se aplica tanto à esfera das provas produzidas no mundo físico como aquelas produzidas em meio digital, e aqui cabe destacar que no ambiente digital a garantia de integridade, confiabilidade e inviolabilidade da cadeia de custódia se apresenta ainda mais importante na medida em que a própria noção e o papel do corpo de delito se altera significativamente além de, como já destacado, quer seja pela dinâmica do desenvolvimento de suas atividades, quer seja pelas possibilidades técnicas e inovações produzidas nesse ambiente,

[1] Adulterar: falsificar, corromper. FERREIRA, Aurélio Buarque de Hollanda, Pequeno Dicionário Brasileiro da Língua Portuguesa, 10ª Edição, Editora Civilização Brasileira S/A, Rio de Janeiro, 1963.
[2] Obliterar: eliminar, suprimir, destruir por completo sem deixar vestígios. FERREIRA, Aurélio Buarque de Hollanda, Pequeno Dicionário Brasileiro da Língua Portuguesa, 10ª Edição, Editora Civilização Brasileira S/A, Rio de Janeiro, 1963.
[3] Ocultar; não deixar ver, não mostrar, não revelar, disfarçar, dissimular, encobrir, esconder. FERREIRA, Aurélio Buarque de Hollanda, Pequeno Dicionário Brasileiro da Língua Portuguesa, 10ª Edição, Editora Civilização Brasileira S/A, Rio de Janeiro, 1963.

a prova qualquer modificação pode se tornar ainda mais difícil. Acerca dessa dinâmica, importante se observar as lições de Ahmed e Roussev (2019, p. 301-302):

> A noção de relevância é inerentemente específica a cada caso e uma grande parte da competência de um analista forense é a capacidade de identificar provas relevantes a um caso. Frequentemente, um componente crítico da análise forense é a atribuição causal de uma sequência de eventos a atores humanos específicos do sistema (tais como usuários e administradores). Quando utilizados em processos judiciais, a proveniência, a confiabilidade e a integridade dos dados utilizados como prova são de suma importância. Em outras palavras, consideramos todos os esforços para realizar análises de sistema ou de artefatos após o fato como uma forma de perícia forense. Isso inclui atividades comuns tais como a resposta a incidentes e investigações internas, que quase nunca resultam em quaisquer processos judiciais. Em geral, somente uma pequena fração das análises forenses chega às salas de audiência como provas formais.[4]

Neste contexto, não é forçoso afirmar que o valor da cadeia de custódia é consideravelmente incrementado quando o elemento probatório possui natureza ou ação digital e se hoje no Brasil há o reconhecimento de que a tutela da autodeterminação informativa deve possuir proteção constitucional especial em decorrência da significativa alteração que os sistemas de Tecnologia de Informação e Comunicação (TIC) ocasionaram (PRADO, 2014), também a legislação infraconstitucional deve caminhar no sentido de evoluir suficientemente para, além de compreender, darem respostas suficientes para os problemas causados pelo seu uso. E é em busca de atingir esses objetivos que as discussões que envolvem o tema cadeia de custódia caminham.

Assim, e uma vez apresentados os principais elementos teóricos da cadeia de custódia no âmbito jurídico-processual, é importante compreender, agora, a relação da Computação Forense (FREITAS; SANTIN, 2015) (FREITAS; SANTIN, 2012) e da criptografia com esse tema. Nesse sentido, partindo-se do pressuposto de que delitos sempre deixam vestígios, é possível compreender que a Computação Forense se destina justamente a solucionar infrações penais desenvolvidas no ambiente digital.

Acerca desse aspecto, Eleutério e Machado (2010, p. 16-17) afirmam que a Computação Forense tem como objetivo determinar "a dinâmica, a materialidade e autoria de

[4] Texto original: "The notion of relevance is inherently case-specific, and a big part of a forensic analyst's expertise is the ability to identify case-relevant evidence. Frequently, a critical component of the forensic analysis is the causal attribution of an event sequence to specific human actors of the system (such as users and administrators). When used in legal proceedings, the provenance, reliability, and integrity of the data used as evidence are of primary importance. In other words, we view all efforts to perform system or artefact analysis after the fact as a form of forensics. This includes common activities such as incident response and internal investigations, which almost never result in any legal actions. On balance, only a tiny fraction of forensic analyses makes it to the courtroom as formal evidence."

ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhes validade probatória em juízo.". Há que se entender, primeiramente, que prova digital é um elemento digital/eletrônico capaz de dar ciência de um fato a alguém. Ou seja, a prova digital encontra sua materialidade em meio digital, representada em sistema binário, por zeros (0) e uns (1), constituindo evidências digitais que podem ser coletadas, armazenadas e analisadas por métodos e técnicas de Computação Forense (ELEUTÉRIO; MACHADO, 2010) (VECCHIA, 2019) (VELHO, 2016). Alguns exemplos de provas digitais são: arquivos de texto, áudios, imagens digitais, planilhas eletrônicas, imagens em qualquer formato, vídeos, registros de logs e operações em sistemas ou redes computacionais, e-mails, mensagens instantâneas, arquivos em CDs, DVDs, nuvem computacional, dispositivos móveis (celulares e *smartphones*), aparatos de jogos eletrônicos e digitais, bancos de dados, bases de dados, entre outros. Esses arquivos eletrônicos, sejam públicos ou particulares, podem ser considerados para fins de direito como documentos digitais (ou eletrônicos), e possuem a natureza de prova documental a que se refere o artigo 212, inciso II do Código Civil (BRASIL, 2002) e, também, os artigos 231 a 238 do Código de Processo Penal (BRASIL, 1941).

Nesse cenário, entende-se que a Ciência Forense e o estudo da cadeia de custódia a partir de provas digitais demandam a compreensão de diferentes técnicas e tecnologias na medida em que, diferente do ambiente físico, o ambiente digital se caracteriza pela existência de uma multiplicidade de fatores de criação e operação. Assim, considerando-se que uma das utilidades do meio digital é o armazenamento de dados e informações, bem como, tendo em mente que dados e formatos de representação em meio digital se apresentam como fontes de garantia e de proteção de conteúdos, o estudo da criptografia tem relevância quando o interesse é garantir a integridade, confiabilidade e veracidade de elementos probatórios em meio digital (PAAR, 2010).

O termo criptografia vem do grego, associando *kriptós* que significa escondido e *gráphein* que significa escrever. Assim, resulta: "escrita escondida". A ideia é poder escrever uma mensagem utilizando uma codificação que somente quem possui uma chave consegue decifrar o que está escrito. Esta ideia não é nova e existe desde o tempo do imperador Júlio César, o qual utilizava um método baseado em substituição, por exemplo com chave igual a 3. Nesse caso, "fdvd" representaria a palavra "casa". Assim, as operações matemáticas de criptografia constituem uma forma específica de tecnologia, a qual pode ser decomposta em duas etapas: a) Criptografar: é a transformação do documento eletrônico em um conjunto

alfanumérico ininteligível; e b) Decriptografar: é o processo inverso, retorno ao documento eletrônico original. Tudo isso pode ser melhor compreendido quando Freitas (2012) já explicava esses procedimentos tecnológicos.

A etapa para criptografar tem por base um algoritmo de dispersão ou função *hash*, constituindo uma sequência de letras e números. O objetivo desta função é identificar um conjunto de informações de maneira unívoca, ou seja, para cada conjunto de informação um único *hash*. Na prática, buscam-se os melhores algoritmos para evitar os problemas clássicos de colisão (*collisions*) (FREITAS, 2012). Isto devido ao fato de que o contra-domínio da função *hash* é menor do que o seu domínio, ou seja, *x* pode assumir uma quantidade muito maior de valores do que *hash*(x). A etapa para decriptografar é, então, o processo inverso. Ou seja, a partir do documento eletrônico criptografado obtém-se o documento original. Os algoritmos que implementam funções *hash* são unidirecionais e não permitem descobrir o conteúdo original a partir do *hash*.

De maneira simples, a criptografia pode ser implementada por algoritmos de criptografia simétrica ou assimétrica. Na criptografia simétrica ou de chave única ou de chave secreta (*secret-key*) existe uma única chave ou código conhecido por ambos os lados envolvidos na transação. A mesma chave opera nas duas etapas (codificação e decodificação). A desvantagem deste método é que somente as partes envolvidas podem ter conhecimento da chave, caso contrário, qualquer outro interessado ou mal-intencionado terá acesso ao conteúdo criptografado, tornando o método vulnerável. Da mesma forma, ao divulgar a chave a todos que necessitam conhecer o documento, também, estar-se-á permitindo que o documento seja acessível e alterável. Fato, não conveniente em determinadas situações, como em provas digitais.

Já a criptografia assimétrica ou de chave pública (*public-key*) é composta por um par de chaves, denominadas chave pública e chave privada. Estas chaves constituem um par de chaves assimétricas, ou seja, diferentes entre si. Sendo a chave privada de propriedade exclusiva do assinante. A vantagem deste processo é a sua segurança, de modo que os algoritmos buscam a geração de chaves da forma mais aleatória possível, garantindo estatisticamente que não se possa nunca repetir o processo para gerar outro par de chaves idêntico, evitando a fraude. Neste processo somente a chave pública é divulgada, por isso a denominação de pública.

O par de chaves é calculado simultaneamente. Isto significa que para uma dada chave privada, só existe uma chave pública que lhe sirva como par. A chave pública pode ser distribuída livremente para todos os interessados. Pode-se divulgar via e-mail, site ou outras formas de divulgação, enquanto a chave privada é de conhecimento apenas do proprietário.

A associação entre a criptografia assimétrica e os mecanismos legislativos visam garantir à assinatura digital diferentes propriedades. As propriedades relevantes são as seguintes e advém da Segurança da Informação normatizada por Norma ISO/IEC 13335-1[5] (FREITAS; SANTOS; PASINATO, 2020, p. 241-242):

a) Autenticidade: é a qualidade de ser autêntico, ou seja, que é do autor a quem se atribui, que faz fé, verdadeiro, certo, genuíno, legalizado. A assinatura é autêntica, pois quando um usuário usa a chave pública de um usuário para decifrar um documento eletrônico, ele confirma que foi esse usuário e somente esse quem assinou o documento. Portanto, a criptografia autentica os arquivos assinados digitalmente.

b) Integridade: a assinatura não pode ser forjada, pois somente o usuário conhece sua própria chave privada e pode aplicá-la, ou seja, somente ele assina o documento eletrônico a ser comunicado, garantindo o conteúdo que consta no arquivo digital até o momento da conferência (contra verificação) com o *hash*;

c) Confiabilidade: é a qualidade de ser confidencial ou, ainda, aquilo que é dito ou escrito em confidência, secreto. O documento assinado não pode ser alterado, pois se houver qualquer alteração no texto criptografado este não poderá ser restaurado com o uso da chave pública. O *hash* é único para cada documento e se houver alteração no conteúdo, a contra verificação do *hash* falhará, demonstrando que o conteúdo foi alterado; e

d) Veracidade: a assinatura tem a presunção de veracidade, pois os demais usuários não necessitam de auxílio do assinante para reconhecer a assinatura de cada assinante em específico e, ainda, o assinante não pode negar ter assinado o documento (irrefutabilidade ou não repúdio). A criptografia foi aplicada e, portanto, não se pode negar a existência do *hash* correspondente ao conteúdo em específico.

Isto posto, é possível sintetizar que a função *hash* é resultado da aplicação da técnica de criptografia apta a garantir a autenticidade, a integridade, confiabilidade e a veracidade do material criptografado. Isso porque eventual alteração na prova digital ocasionará alteração no próprio *hash*, cuja ausência de correspondência com o *hash* original demonstra que a cadeia de custódia foi violada. Ou seja, a incolumidade do *hash* demonstra a incolumidade da prova e, com isso, da própria cadeia de custódia, restando preservadas as garantias processuais constitucionais dos implicados no caso penal.

[5] ISO/IEC 1333-1. Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management. 2004. p. 03. Disponível em https://www.iso.org/standard/39066.html Acesso em 19 out. 2022.

Portanto, do ponto de vista da cadeia de custódia de evidências digitais, a citada técnica aplicável na área de Computação Forense mostra-se indispensável à sua preservação. Afinal, a cadeia de custódia, do posto de vista técnico da Computação Forense, visa "à garantia de integridade do material encontrado em uma investigação" e, portanto, consiste numa "sequência de proteção e guarda (custódia) dos elementos materiais encontrados durante uma investigação e que devem manter as suas características originais e informações íntegras, sem deixar dúvidas sobre a sua origem e manuseios realizados" (VECCHIA, 2019, p. 100).

Há que se lembrar que todo esses procedimentos devem ser registrados na cadeia de custódia, de modo cronológico, registrando-se passo a passo desde a coleta até o descarte do conjunto probatório, passando-se obrigatoriamente pelas de identificação, isolamento, coleta, armazenamento e preservação, exames e análises, visando a obtenção dos resultados (VELHO, 2016, p. 18-35) a serem registrados em laudo pericial (VELHO, 2016, p. 565-593).

Diante de todo esse cenário, e demonstrado que a criptografia se apresenta como ferramenta apta a tornar o conjunto probatório idôneo, na medida em que vai além da codificação dos conteúdos digitais, gerando o *hash* correspondente, fica evidente a sua importância para a cadeia de custódia, na medida em que seu emprego se apresenta como condição essencial para a garantia da integridade, inviolabilidade e autenticidade da evidência probatória coletada em meio digital.

4. REFLEXOS E VANTAGENS DO USO DA CRIPTOGRAFIA NA CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS

Considerando-se o exposto sobre as características técnicas da criptografia, entende-se que tais características são essenciais a formação, manutenção e manuseio das diferentes fases da cadeia de custódia. Por exemplo, no isolamento, fase essa necessária para "evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime" (BRASIL, 2019), a criptografia poderá garantir a documentação do correto isolamento do local, por meio de imagens digitais e seus metadados. Já no acondicionamento, na medida em que esse procedimento se caracteriza por ser o meio pelo qual cada vestígio coletado é embalado de modo a ser posteriormente analisado, a criptografia com geração do *hash* permitirá a autenticidade do espelhamento dos dados coletados. E, durante, a etapa de processamento, na medida em que a manipulação poderá ser controlada e preservada de acessos não autorizados, a criptografia e o *hash* garantirão a integridade dos dados a serem analisados. E, por fim, a criptografia e o *hash* garantiram ao

armazenamento do conjunto probatório todas as propriedades advindas da Segurança da Informação, uma vez que o elemento probatório poderá ser armazenado de modo a se evitar acessos indevidos e não controlados.

Afora isso, a utilização de *hash* na cadeia de custódia de provas digitais terá papel preponderante na medida em que ele será responsável por estabelecer uma relação unívoca entre a evidência digital e o *hash* propriamente dito, ou seja, será possível conferir a determinado material digital probatória as seguintes garantias: a) o arquivo imageado e criptografado está íntegro; b) os peritos (oficiais ou nomeados), ao realizarem as análises, não introduziram mudanças nas informações coletadas/colhidas; e c) o processo de coleta/colheita, e até mesmo de produção antecipada de provas digitais, foi realizado corretamente.

Há que se mencionar que mesmo obtendo-se o *hash* das provas digitais, não se pode dispensar as demais exigências técnico-científicas em relação aos procedimentos de cadeia de custódia, a saber: a) Obter o *hash* do material original antes de realizar o procedimento de imageamento; b) Após o imageamento do material original, obter o *hash* do material imageado e compará-lo com o *hash* do material original. O material imageado será o material de análise; c) É necessário que, além do material imageado, seja obtida também uma cópia que deverá ser lacrada para o uso em caso qualquer questionamento técnico ou jurídico das partes; d) A cada novo acesso ou ação com as cópias provenientes das provas digitais, deve-se registrar o responsável pelo acesso, a data e o horário, bem como os procedimentos aplicados.

Apesar disso, e de sua relevância e importância tanto para a Ciência Forense quanto para o Direito, a disseminação, implantação e operacionalização dessa tecnologia entre peritos e profissionais envolvidos na cadeia de custódia – juízes, advogados, promotores, assistentes técnicos, entre outros; tem esbarrado na falta de conhecimento sobre sua existência e forma de operação, assim como, "na necessidade de escolha consciente de se empregar tal técnica, e na dificuldade de implementação correta pelo público leigo em Segurança da Informação" (ABREU, 2017, p. 12). E esse desconhecimento faz com que, inclusive, medidas extraordinárias que não tem efeito prático algum sejam tomadas por magistrados, como foi o caso das determinações judiciais que suspenderam o uso do aplicativo de mensagens WhatsApp no Brasil.[6]

[6] Foram várias as decisões judiciais que tiveram como objetivo derrubar ou inoperacionalizar o aplicativo de mensagens WhatsApp, medidas estas tomadas sempre com base na suposta omissão da empresa que se recusava a disponibilizar para as autoridades policiais o conteúdo das mensagens trocadas por determinados indivíduos. A questão se tornou tão relevante que motivou a Ação Direta de Inconstitucionalidade nº 5.527 e a Arguição de Descumprimento de Preceito Fundamental nº 403 que foram objetivo de discussão por parte do Supremo Tribunal Federal (STF). Para maiores informações acerca das impossibilidades técnicas envolvidas nesses pedidos consultar: FERRAZ JUNIOR, Tercio Sampaio; MARANHÃO, Juliano; FINGER, Marcelo. O desafio do

E em um cenário em que a justiça expede diariamente dezenas de milhares[7] de mandados e ofícios que têm por objetivo produzir provas advindas do meio digital, tais como, interceptação telefônica e telemática; apreensão de computadores, celulares e outros dispositivos móveis; gravação de vídeos ou sons; e tantas outra ações que tem como objetivo apreender ou ter acesso a determinadas comunicações; se faz de extrema importância as discussões que levem ao conhecimento e maior emprego dessa técnica.

E não adianta buscar a imputação das próprias empresas de TIC pela obrigatoriedade de desenvolver mecanismos que sejam capazes de possibilitar o emprego de ferramentas de criptografia em suas atividades ou de auxiliarem os órgãos de justiça nesse sentido, e isso se dá por vários motivos, mas em especial: a) Impossibilidade técnica de garantia de controle de acesso à comunicação criptografada, na medida em que diferentes atores estarão envolvidos no processo de criptografia; e b) Falta de normativa legal que autorize tal ação por parte de entes públicos, sendo importante lembrar que o Marco Civil da Internet não instituiu, ao menos não explicitamente, nenhuma obrigação as empresas de tecnologia de abrirem ou exporem as suas técnicas de criptografia. Mas, por outro lado, com o advento da Lei Geral de Proteção de Dados Pessoais (LGPD), consta como direito dos titulares de dados, artigo 18, inciso II, o direito de obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição, o acesso aos dados pessoais, incluindo-se os dados pessoais sensíveis (BRASIL, 2018).

Por fim, importa destacar que mesmo sendo demonstrada e evidenciada a importância e a imprescindibilidade da aplicação de técnicas de criptografia na cadeia de custódia de provas digitais, ainda assim tais fatores não são suficientes para ensejar que o Estado busque incentivar o seu uso à partir da sua normatização, e acerca desse aspecto – da normatização do desenvolvimento, uso e emprego da criptografia, Abreu (2017, p. 39) destaca que:

> [...] cabe lembrar que somente é possível um debate racional sobre essas questões de política regulatória se ele for informado — baseado em evidências concretas, não em casos anedóticos e retórica do medo. Para falar que criptografia está realmente comprometendo investigações e a segurança pública em geral de uma forma que legitime a regulamentação de alguma forma, seria necessário um levantamento de evidência empírica robusta sobre todas as vezes em que essa dificuldade foi crítica

WhatsApp ao Leviatã. *Folha de S. Paulo*, São Paulo, 16 ago. 2016. Opinião. Disponível em http://www1.folha.uol.com.br/opiniao/2016/08/1803323- o-desafio-do-whatsapp-ao-leviata.shtml;. Acesso em 19 out. 2022. VOLPI NETO, Angelo; FREITAS, Cinthia Obladen de Almendra Freitas. Whatsapp e o Bloqueio. Information Management, Editora Guia: São Paulo, p. 54 - 55, publicado em: 02-maio-2016.

[7] Apenas no ano de 2015, e unicamente em relação à pedidos de interceptação telefônica ou telemática, foram expedidos mais de 100.568 ofícios. Para maiores informações consultar: CONSELHO NACIONAL DE JUSTIÇA. Sistema Nacional de Controle de Interceptações. Disponível em: http://www.cnj.jus.br/interceptacoes_tel/relatorio_quantitativos.php. Acesso em: 21 out. 2022.

> para a não resolução de um caso, conjuntamente com levantamento de dados sobre qual tipo de crime se tratava. Semelhantemente, para julgar potenciais alternativas regulatórias, é imprescindível uma séria avaliação de riscos para a cibersegurança individual, coletiva e nacional e para direitos humanos, discussão sobre viabilidade e operacionalização do modelo a nível global, efetividade da medida e impacto no mercado. Será importante, também, levar em conta o efeito colateral da utilização (e permissão) da criptografia forte na investida em técnicas de investigação via hacking estatal, tema que, também, desperta questões peculiares de privacidade e segurança. Tudo isso dentro de um contexto regulatório que pode se alterar profundamente com o desenvolvimento tecnológico, como por exemplo pela eventual descoberta e disseminação de formas inovadoras de criptoanálise a serem exploradas por autoridades de segurança.

Ou seja, o aumento no uso e emprego de técnicas de criptografia no âmbito da cadeia de custódia deverá vir pela compreensão dessa tecnologia e sua difusão. Ainda, e mesmo que o Superior Tribunal de Justiça mantenha seu entendimento, a inviolabilidade continuará sendo a guia mestre no que se refere a formação e preservação da cadeia de custódia, sem contar é claro no fato de que, de posse dessa tecnologia, peritos, assistentes técnicos, advogados, juízes e promotores poderão desempenhar de forma célere e satisfatória suas funções.

5. CONSIDERAÇÕES FINAIS

O artigo enfrentou aspectos jurídicos e tecnológicos da cadeia de custódia de provas digitais, questionando se: a criptografia pode ser utilizada para conferir maior proteção às provas digitais no contexto da cadeia de custódia? Para tal, fez-se uso do método de pesquisa hipotético-dedutivo, apoiando-se em técnicas de pesquisa bibliográfica e legislativa. Tem-se como premissas a prova documental e o "Pacote Anticrime", Lei nº 13.964 de 24 de dezembro de 2019, que instituiu a cadeia de custódia no Processo Penal, trazendo à discussão a preservação e devida manipulação da prova processual no âmbito penal. Mas restou insuficiente a instrumentalização de procedimento para cadeia de custódia de provas em meio digital, ou mesmo. Novamente, confronta-se o mundo físico e analógico com o mundo digital.

O artigo apresenta os aspectos e as nuances da cadeia de custódia no contexto brasileiro e aprofunda a discussão dos aspectos tecnológicos da aplicação da criptografia na cadeia de custódia de provas digitais, apontando os reflexos e as vantagens do uso da criptografia nesse contexto.

Relaciona-se a Computação Forense com a aplicação da criptografia de modo a conferir propriedades da Segurança da Informação, a saber: autenticidade, integridade, confiabilidade, veracidade e irrefutabilidade ou não repúdio. Cabe ao *hash*, resultado da operação de criptografia de conteúdos digitais, conferir uma relação unívoca entre conteúdo e

código *hash*, propriamente dito. Qualquer eventual alteração na prova digital ocasionará alteração no próprio *hash*, cuja ausência de correspondência com o *hash* original demonstra que a cadeia de custódia foi violada. Ou seja, a incolumidade do *hash* demonstra a incolumidade da prova e, com isso, da própria cadeia de custódia, restando preservadas as garantias processuais constitucionais dos implicados no caso penal.

Finalmente, conclui-se que em sendo as provas digitais há que se lançar mão de tecnologias digitais para garantir propriedades imprescindíveis à essa categoria de prova documental, conferindo transparência e idoneidade, não somente às provas, mas também a todo o procedimento de cadeia de custódia.

REFERÊNCIAS

ABREU, Jaqueline de Souza. **Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação**. Revista Brasileira de Política Públicas. Vol. 7, Nº 3, dez., 2017.

AHMED, Irfan; ROUSSEV, Vassil. Analysis of Cloud Digital Evidence. In: CHEN, Lei; TAKABI, Hassan; LE-KHAC, Nhien-An (ed.). Security, Privacy, and Digital Forensics in the Cloud. Hoboken, Singapura: John Wiley & Sons, 2019. p.301-302.

BRASIL. **Constituição da República Federativa do Brasil**, 1988. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 19 out. 2022.

BRASIL**, Lei Nº 13.964, de 24 de dezembro de 2019**, Aperfeiçoa a legislação penal e processual penal, 2019. Brasília: DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 19 out. 2022.

BRASIL**, Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD**, 2018. Brasília: DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 out. 2022.

BRASIL. **Código Civil**, **Lei Nº 10.406, de 10 de janeiro de 2002.** Brasília: DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 19 out. 2022.

BRASIL. **Decreto-lei Nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 19 out. 2022.

BRASIL. Superior Tribunal de Justiça. *Habeas Corpus* nº 160.662/RJ – Rio de Janeiro. Relatora: Ministra Assusete Magalhães, Sexta Turma, julgado em 18/02/2014, DJe de 17/03/2014. **Jurisprudência do STJ.** Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/864482320/inteiro-teor-864482321. Acesso em: 19 out. 2022.

BRASIL. Superior Tribunal de Justiça. *Habeas Corpus* nº 653.515 - RJ (2021/0083108-7) – Rio de Janeiro. Relator: Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 23/11/2021, DJe de 01/02/2022. **Jurisprudência do STJ.** Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1365911352/inteiro-teor-1365911896. Acesso em 19 out. 2022.

CARVALHO, Luis Gustavo Grandinetti Castanho de. **Processo Penal e Constituição: princípios constitucionais do processo penal**. São Paulo: Editora Saraiva, 2014. *E-book*.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Márcio Pereira. **Desvendando a Computação Forense.** São Paulo: Novatec Editora, 2010.

FREITAS, Cinthia Obladen de Almendra Freitas; SANTOS, Henrique Guilherme; PASINATO, Rita. **A Segurança da Informação como Ferramental Técnico da Proteção de Dados Pessoais**. In: Mariana Pereira Faria; Rafael Aggens Ferreira da Silva; Rhodrigo Deda Gomes. (Org.). Direito e Inovação - Volume 3. 1ed.Curitiba: NCA - Comunicação e Editora LTDA, 2020, v. 3, p. 233-265.

FREITAS, Cinthia Obladen de Almendra Freitas; SANTIN, Altair Olivo. **Forense Computacional**. In: Rodrigo Grazinoli Garrido;Alexandre Giovanelli. (Org.). Ciência Forense: uma introdução à criminalística (2a. edição revisada e ampliada). 2ed.Rio de Janeiro: Projeto Cultural, 2015, v. 1, p. 195-199.

FREITAS, Cinthia Obladen de Almendra Freitas; SANTIN, Altair Olivo. **Computação Forense**. In: Rodrigo Grazinoli Garrigo;Alexandre Giovanelli. (Org.). Ciência Forense: Uma Introdução à Criminalística. 1ed.Rio de Janeiro: FAPERJ, 2012, v. 1, p. 165-170.

FREITAS, Cinthia Obladen de Almendra Freitas. **Assinatura Digital**: Necessidade ou Obrigação?. In: Antônio Carlos Efing; Cinthia O. de A. Freitas. (Org.). Direito e Questões Tecnológicas - Aplicados no Desenvolvimento Social. 1ed.Curitiba: Editora Juruá, 2008, v. 1, p. 131-155.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**: Volume Único. 8. ed. rev. atual. e aum. Salvador: Juspodivm, 2020.

LOPES JÚNIOR, Aury. **Direito processual penal**. 19. Ed. São Paulo: Saraiva, 2022. *E-book*.

PAAR, Christof; PELZL, Jan. **Understanding cryptography: a textbook for students and practitioners**. London: Springer, 2010.

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

VECCHIA, Evandro Dalla. **Perícia Digital:** da investigação à análise forense. 2 ed. Campinas: Millenium Editora, 2019.

VELHO, Jesus Antonio. **Tratado de Computação Forense**. Jesus Antonio Velho (Org.). Campina, SP: Millennium Editora, 2016.