UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB
CENTRO DE CIÊNCIAS JURÍDICAS – CCJ
COORDENAÇÃO DO CURSO DE DIREITO – CAMPUS JOÃO PESSOA
COORDENAÇÃO DE MONOGRAFIA

FERNANDA SILVA DE LIMA

TRATAMENTO DA PROVA DIGITAL E A GARANTIA DA AUTENTICIDADE À LUZ DO DIREITO E DA TECNOLOGIA

JOÃO PESSOA
2022

FERNANDA SILVA DE LIMA

TRATAMENTO DA PROVA DIGITAL E A GARANTIA DA AUTENTICIDADE À LUZ DO DIREITO E DA TECNOLOGIA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientadora: Profa Dra. Larissa Teixeira Menezes de Freitas

JOÃO PESSOA
2022

Catalogação na publicação
Seção de Catalogação e Classificação

L732t Lima, Fernanda Silva de.
Tratamento da prova digital e a garantia da autenticidade à luz do direito e da tecnologia / Fernanda Silva de Lima. - João Pessoa, 2022.
52f.

Orientação:Larissa freitas.
Monografia (Graduação) - UFPB/CCJ.

1. Cadeia de custódia. 2. Registro digitais. 3. VERIFACT. I. Freitas, Larissa. II. Título.

UFPB/CCJ CDU 34

FERNANDA SILVA DE LIMA

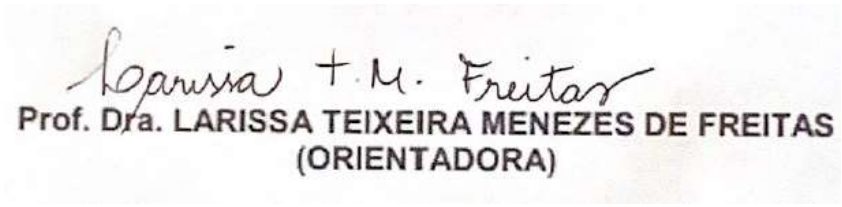
TRATAMENTO DA PROVA DIGITAL E A GARANTIA DA AUTENTICIDADE À LUZ DO DIREITO E DA TECNOLOGIA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientador: Profa. Dra. Larissa Teixeira Menezes de Freitas

DATA DA APROVAÇÃO: 15 DE JUNHO DE 2022

BANCA EXAMINADORA:



(AVALIADORA)

(AVALIADORA)

AGRADECIMENTOS

A Jesus Cristo, a luz que guia a minha vida e me toma de felicidade, a Deus, pela misericórdia e o amor que me sustenta, a Nossa Senhora, minha mãezinha do céu e minha intercessora, a todos os anjos e santos que desde a minha infância são meu refúgio, e ao universo, que com sua imensidão me permiti ser um pequeno grão de areia que junto com os demais nos faz perceber que o ser humano precisa viver em harmonia com o que nos cerca para que façamos parte do todo.

Agradeço aos meus pais, Maria das Neves e Francisco, que, com amor e simplicidade, fizeram-me perceber que a felicidade está em mim e não nas coisas materiais e pessoas que me rodeiam. A vocês, minha gratidão eterna.

Ao meu esposo Silvio, amigo e companheiro que me desafia diariamente a superar meus limites, e a trazer para o meu dia a dia, uma frase de William Shakespear: *"E você aprende que realmente pode suportar. Que realmente é forte e que pode ir muito mais longe, depois de pensar que não se pode mais".*

As minhas irmãs, Flávia e Fabiana, que juntas aprendemos a amar, a compartilhar, a aceitarmos as diferenças, a superarmos obstáculos e a lutarmos, com a certeza de que independentemente do que aconteça em nossas vidas, teremos sempre umas às outras.

A minha filha, Letícia, a razão e a luz da minha vida e de todas as minhas conquistas, um pedaço de mim, que me permitirá viver eternamente através dos seus filhos, netos e demais descendentes.

Aos meus sobrinhos, Gabriel e João Miguel, e ao meu afilhado, Davi, meus pequenos príncipes que amo e me enchem de motivos para sorrir.

A minha orientadora, Larissa Teixeira, que com toda presteza, sabedoria e humildade, esteve presente durante toda a construção deste trabalho, sendo fundamental para sua concretização.

Em tempo, quero agradecer aos meus cunhados, Jean e Emerson, aos meus enteados, Thiago e Thaina, e a todos os meus amigos, presentes em minha vida, com quem compartilho tristezas e alegrias, e que me fazem perceber que a família é muito além do laço de sangue, pois temos a dádiva de escolhermos e sermos escolhidos, tornando os meus dias mais felizes.

RESUMO

O presente estudo objetivou analisar os desafios e dilemas enfrentados com a evolução tecnológica e o uso cotidiano dos ambientes virtuais, que alterou a forma de relacionamento entre as pessoas, o trabalho, tal como a seara processual. Neste período de insegurança e transformações, cabe refletir sobre a importância do cumprimento dos passos essenciais que devem ser executados na coleta de registros digitais como meio de assegurar a autenticidade de documentos eletrônicos. Alguns dos caminhos galgados foi explicar o que são fatos jurídicos, provas, como um documento eletrônico pode ser um meio de prova digital, bem como, identificar as principais características e cuidados com provas digitais, apresentando os passos essenciais da cadeia de custódia digital que devem ser executados na coleta de registros digitais, conferindo segurança a prova produzida e dirimindo controvérsias; conhecer ferramenta de coleta de metadados detalhados de fatos digitais que pode garantir integridade, confiabilidade, auditabilidade da prova digital e a sua credibilidade para aceitação em juízo. Para tal finalidade, foi disposto como método para coleta de dados a pesquisa bibliográfica e documental, através do estudo levantado no referencial teórico sobre como garantir a autenticidade probatória ao documento eletrônico, por meio do cumprimento das etapas essenciais que devem ser executadas na coleta dos registros digitais. Doravante da análise de dados foi possível perceber a relevância em adequar o direito às inovações da sociedade, à produção de provas no meio eletrônico, tendo em vista que estas impactam diretamente nas ações e decisões judiciais. A execução da coleta de registros digitais se impõe como meio de garantir a autenticidade probatória à prova digital. A falta de uma padronização legal em relação a cadeia de custódia das provas digitais de forma a abranger qualquer fonte de prova de natureza real, apresenta-se como o maior desafio para aceitação da prova digital em juízo, pois a evidência digital pode ser facilmente manipulada, dificultando a resolução de crimes em ambientes digitais, e gerando insegurança jurídica. Em suma, por meio de todo o estudo realizado foi possível confirmar que a prova digital é vulnerável à adulteração, sua autenticação é fundada por métodos técnico científicos, e o cumprimento das 03 (três) fases fundamentais durante a coleta e conservação da prova digital: Isolamento, Coleta técnica detalhada e Preservação, permitem assegurar a autenticidade de documentos eletrônicos, o que possibilita meios de prova digital de credibilidade e maior proximidade da verdade real dos fatos. No mercado podem ser encontradas ferramentas, a exemplo da VERIFACT, que é capaz de viabilizar uma verificação esclarecedora do fato ocorrido em ambiente digital, e, ao mesmo tempo, proteger a prova de fraudes e manipulações, cumprindo a Cadeia de Custódia digital e atendendo tecnicamente as diretrizes de confiança da coleta e preservação dos registros de evidências digitais.

Palavras-chave: Cadeia de custódia. Registros digitais. VERIFACT.

ABSTRACT

The present study aimed to analyze the challenges and dilemmas faced with technological evolution and the virtual environments daily use, which have changed the form of relationships between people, work, as well as the procedural field. In this period of insecurity and transformations, it is important to reflect on the importance of complying with the essential steps that must be taken in the collection of digital records as a means of ensuring the authenticity of electronic documents. Some of the paths taken were to explain what legal facts and evidence are and how an electronic document can be a means of digital evidence, as well as to identify the main characteristics and care with digital evidence, presenting the essential steps in the digital chain of custody that must be performed in the collection of digital records, providing security to the evidence produced and settling controversies; and get to know a detailed metadata collection tool of digital facts that can guarantee integrity, reliability and auditability of digital evidence and its credibility for acceptance in the court. For this purpose, bibliographic and documentary research was used as a method for data collection, through the study raised in the theoretical framework on how to guarantee the probative authenticity of the electronic document, through the fulfillment of the essential steps that must be performed in the collection of digital records. Henceforth, from the data analysis, it was possible to perceive the relevance of adapting the law to society's innovations, and the evidence production in electronic environment, given that these directly impact judicial actions and decisions. The execution of the collection of digital records is imposed as a means of guaranteeing the probative authenticity of digital evidence. The lack of legal standardization regarding the chain of custody of digital evidence in order to cover any source of a real nature's evidence, presents itself as the biggest challenge for the acceptance of digital evidence in court, as digital evidence can be easily manipulated, making it difficult to solve crimes in digital environments, and generating legal uncertainty. In short, through the entire study carried out, it was possible to confirm that digital evidence is vulnerable to tampering, its authentication is based on technical-scientific methods, and compliance with the 03 (three) fundamental phases during the collection and conservation of digital evidence: Isolation, Detailed Technical Collection and Preservation, allow ensuring the authenticity of electronic documents, which allows for credible digital evidence and greater proximity to the real truth of the facts. Tools can be found on the market, such as VERIFACT, which is capable to enabling an enlightening verification of the fact that occurred in a digital environment, and, at the same time, protecting proof of fraud and manipulation, complying with the digital Chain of Custody and technically the trust guidelines for the collection and preservation of digital evidence records.

Keywords: Chain of custody. Digital records. VERIFACT.

SUMÁRIO

1 INTRODUÇÃO 7
2.1 VISÃO SOBRE FATOS JURÍDICOS 9
2.2 MEIOS DE PROVA 10
2.3 DOCUMENTO ELETRÔNICO COMO MEIO DE PROVA DIGITAL NA ATUALIDADE 12
3 CADEIA DE CUSTÓDIA E A COLETA DE PROVAS DIGITAIS NA ATUALIDADE 15
3.1 DA CADEIA DE CUSTÓDIA 15
3.2 DA CADEIA DE CUSTÓDIA DAS PROVAS DIGITAIS 20
3.3 FRAGILIDADE DA COLETA DAS PROVAS DIGITAIS EM RELAÇÃO A AUTENTICIDADE PROBATÓRIA 23
4 FERRAMENTA DE COLETA DE REGISTROS DIGITAIS PARA FINS JUDICIAIS 29
4.1 ETAPAS ESSENCIAIS PARA A COLETA E PRESERVAÇÃO DA PROVA DIGITAL 29
4.2 FERRAMENTA *VERIFACT* X *BLOCKCHAIN* COMO PROVA DIGITAL CONFIÁVEL 32
4.3 CREDIBILIDADE PARA ACEITAÇÃO EM JUÍZO DO RELATÓRIO TÉCNICO EMITIDO POR FERRAMENTA DE COLETA DE METADADOS DE FATOS DIGITAIS 36
5 CONSIDERAÇÕES FINAIS 45
REFERÊNCIAS 48

1 INTRODUÇÃO

A evolução tecnológica trouxe para a sociedade o uso cotidiano dos ambientes virtuais, modificando a forma de relacionamento entre as pessoas, a forma de trabalho, bem como a seara processual. Pois os registros criados ou transmitidos em meio eletrônico, vem sendo utilizado como meio de prova em ações judiciais, e em se tratando de um meio de prova moderadamente novo, a utilização dos registros eletrônicos gera grandes discussões.

Neste diapasão, diante da importância do tema e a carência de adequação do direito às inovações da sociedade, a produção de provas no meio eletrônico ganha destaque dentro dos avanços sociais e tecnológicos e por consequência impacta diretamente nas ações e decisões judiciais, tornando-se primordial reconsiderar o padrão habitual de produção de provas, atualmente ancorada principalmente na oitiva de testemunhas.

A prova adquirida a partir de documentos não formais necessita de métodos técnicos que proporcionem garantir um material probatório confiável, utilizando registros digitais para auxiliar magistrados, advogados e partes na instrução processual, diretamente na produção de provas para dirimir aspectos controvertidos, e almejando-se uma maior agilidade à tramitação processual e maior proximidade da verdade real dos fatos.

O objetivo geral busca apresentar os passos essenciais que devem ser executados na coleta de registros digitais como meio de assegurar a autenticidade de documentos eletrônicos e responder a problemática de como a execução da coleta de registros digitais pode garantir a autenticidade probatória à prova digital.

Para averiguar o tratamento da prova digital como garantia de sua autenticidade como prova não documental, a pesquisa envolveu uma revisão bibliográfica sobre temas correlatos, tais como fatos jurídicos, registros digitais, cadeia de custódia da prova e analise de uma ferramenta de coleta de metadados/registros digitais. Contemplou, ainda, uma pesquisa documental através de uma busca aos Tribunais brasileiros, mais precisamente ao Superior Tribunal de Justiça (STJ) e Supremo Tribunal Federal (STF), para analisar os caminhos escolhidos pela jurisprudência para tratar essa atual prova não documental. Realizou-se a busca acessando os sites do Tribunais e utilizando palavras chaves como “provas digitais” e “cadeia de custódia”.

O objetivo da pesquisa é atingido com os três capítulos a seguir. O primeiro apresenta uma visão sobre fatos jurídicos, prova e meios de prova em direito, bem como uma explicação sobre documento eletrônico como meio de prova digital e sua relevância para externar a ocorrência ou a verdade dos fatos alegados.

No capítulo seguinte, discorre-se sobre a cadeia de custódia da prova, observando que, em regra, prevalece o impedimento do uso da prova ilícita no sistema normativo jurídico brasileiro, da mesma forma, são aceitas todas as formas de prova, desde que legal ou moralmente legítimas, neste sentido, é válida a prova adquirida por meio eletrônico. No entanto, com vistas a garantir a validade da prova digital, durante a sua coleta é necessária a preservação da cadeia de custódia.

Nesse diapasão será abordado o conceito de cadeia de custódia suas etapas, e sua definição diante da Lei n.º 13.964/2019, com vistas a reconhecer a importância do uso da cadeia de custódia do processo penal em dados digitais, desde a sua coleta até o uso como meio de prova, será analisado também a legislação brasileira em relação aos possíveis dispositivos de introdução da cadeia de custódia das provas digitais. Abordar a aplicação dos princípios relativos a cadeia de custódia da prova digital, em busca de evitar a sua contaminação e consequente ilicitude.

Tratar das fragilidades das provas digitais, trazendo algumas decisões judiciais nesse sentido. Enfrentar alguns obstáculos em relação a admissibilidade do documento eletrônico como prova. Debater a fragilidade da Ata notarial, que é um meio legal de prova, mas como meio de formação de prova digital não cumpre as etapas da cadeia de custódia.

Por fim, no terceiro capítulo será enfrentada as fases essenciais de coleta e preservação da cadeia de custódia da prova digital. Apresentar o funcionamento de uma ferramenta que coleta dados digitais e que se encontra em uso no mercado, abordando se a ferramenta cumpre as etapas essenciais para a coleta e preservação da prova digital, em harmonia com às normas internacionais (ABNT NBR ISO/IEC 27037:2013), do ponto de vista técnico, comparando brevemente a ferramenta e o Blockchain. Será analisada a aceitação da prova digital decorrente dessa ferramenta pelo judiciário brasileiro.

2 DOS FATOS JURÍDICOS E PROVAS

Como a vida em sociedade nos permite vivenciar situações que implicam em consequências que norteiam a esfera do direito, temos os fatos jurídicos, que precisam por meio legal demonstrar através das provas a verdade alegada, com vista ao convencimento do juiz a respeito da reconstrução da situação jurídica manifestada, de forma a dirimir controvérsias.

2.1 VISÃO SOBRE FATOS JURÍDICOS

Segundo Miguel Reale (2001) fatos jurídicos são acontecimentos humanos ou naturais, alvos de valorações humanas, que passaram a ser juridicamente qualificados, ou seja, um evento que foi codificado, tipificado e objetivado pelo direito. Como bem nos assegura Pontes de Miranda (2000), fato jurídico é aquele em que a norma abstrata incide sobre ele, dando-lhe cor, e fazendo-o “jurídicos”.

Para Gagliano, Pamplona Filho (2019) fato jurídico facilita, determina a ocorrência de efeitos que modificam, constituem, ou extingue direitos e obrigações no âmbito do direito: “Indiscutivelmente, trata-se de conceito basilar, verdadeira causa genética das relações jurídicas, e, bem assim, dos direitos e obrigações aí compreendidos. Fora da noção de fato jurídico, pouca coisa existe ou importa para o direito” (GAGLIANO; PAMPLONA, 2019, p.161).

Conforme apontado acima, fato jurídico é aplicado quando um evento, seja ele decorrente da natureza ou de ação humana, é evidenciado pelo direito, melhor dizendo, fato jurídico são acontecimentos que reverbera consequências na ciência jurídica. Claramente a aplicação pode ser empregada com vistas a identificar os acontecimentos da vida que tenham relevância para o ordenamento jurídico.

Para que seja verificado se um dado acontecimento pode assim ser determinado como fato jurídico, faz-se necessário observar a situação com a lente do direito. Cita-se, como exemplo, um caso em que um raio venha a cair em determinado lugar, isso não ensejará um fato jurídico, mas se esse raio ao cair atingiu várias residências que ficavam próximas, causando mortes e destruição de bens, há agora um fato jurídico, não em virtude do raio, mas a situação gerada por ele.

Ainda para Gagliano e Pamplona:

> A noção de fato jurídico, entendido como o evento concretizador da hipótese contida na norma, comporta, em seu campo de abrangência, não apenas os acontecimentos naturais (fato jurídico em sentido estrito), mas também as ações humanas lícitas ou ilícitas (ato jurídico em sentido amplo, que se subdivide em negócio jurídico e em ato jurídico stricto sensu; e ato ilícito, respectivamente), bem como aqueles fatos em que, embora haja atuação humana, está é desprovida de manifestação de vontade, mas mesmo assim produz efeitos jurídicos (ato-fato jurídico) (GAGLIANO; PAMPLONA, 2019, p.161).

Nesse sentido, fato jurídico permite a aquisição, a extinção ou alteração de direitos e obrigações. Logo, é importante compreender que todo episódio importante para o direito e passível de ser regulado por uma norma jurídica é um fato jurídico, podendo o mesmo desdobrar-se de uma ação pessoal ou um evento natural. Destarte, exemplificando fato jurídico com o óbito de uma pessoa, este é um fato natural que tem como consequência um fato jurídico, e firma o término da personalidade jurídica; porém, quando falamos de um contrato de aluguel de imóvel, que é firmado de acordo com a vontade das partes, este é um fato jurídico gerado pela conduta humana.

2.2 MEIOS DE PROVA

Segundo Theodoro Júnior (2015) prova é elemento fundamental para se fazer Justiça, e sua importância sequer é questionada. Em especial nos litígios de ordem civil, a prova na grande maioria dos casos é o único caminho de se chegar aos fatos tal como ocorreram, buscando formar o convencimento do juiz com base em fatos concretos e comprovados.

Como bem nos assegura Azevedo (2007), prova como a origem da prova, é no sentido de gênese, de fonte de prova, de concepção onde a mesma brota. Existe também, a prova como instrumento de prova, que se trata da técnica de se remover a prova de sua origem e transferi-la para o processo de modo a possibilitar que o magistrado conheça a verdade dos fatos alegados e apresentados em juízo pelas partes para sua apreciação, com vistas a embasar seu convencimento; e ainda a prova em sentido subjetivo, como resultado, isto é, quando decorrente da confiança depositada na prova produzida nos autos do processo, o julgador chega na sua decisão.

Para Almeida e Faria (2015), prova facilita elucidar os fatos e questões envolvidas na demanda, motivo pelo qual deve a instrução probatória ser cercada de

cuidados, entre eles o saneamento do processo de forma a delimitar as questões e distribuir o ônus da prova:

> O papel da prova na demanda judicial é levar ao magistrado o conhecimento dos fatos de forma que o julgamento ocorra o mais preciso e o mais próximo possível da realidade fática. Isto porque ex facto oritur jus, ou seja, todo direito concebido e garantido pela lei deverá decorrer de determinados fatos que formam aquele direito. Desta forma, o direito à prova é garantia fundamental das partes, derivando do direito ao contraditório, a ampla defesa e do acesso à justiça (ALMEIDA; FARIA, 2015, p. 66).

Como se pode verificar nessa citação, a prova é de relevância inquestionável, é o meio de se alcançar a necessária cognição dos fatos ocorridos e das pretensões litigiosas. Evidentemente a aplicação pode ser utilizada para o esclarecimento e comprovação dos fatos, com vistas que a sentença proferida reflita a mais correta e precisa realidade dos fatos.

É elemento fundamental para se fazer Justiça, e sua importância sequer é questionada. Em especial nos litígios de ordem civil, a prova na grande maioria dos casos é o único caminho de se chegar aos fatos tal como ocorreram, buscando formar o convencimento do Juiz com base em fatos concretos e comprovados. Cita-se, como exemplo, o constante no art. 357 do Código de Processo Civil de 2015, os meios de prova devem ser especificados na fase de saneamento e organização do processo. Os meios de prova admitidos pelo direito são os mais diversos, como o documental, o pericial, o testemunhal, entre outros (BRASIL, 2015).

Ainda para Almeida e Faria:

> Quanto a sua posição sistemática, a prova corresponde a um direito processual e não material. Essa se destina a preparar o processo para o julgamento e representa um direito constitucionalmente garantido, como uma das vertentes do devido processo legal. A prova não se destina a provar fatos, mas as afirmações desses; destina-se a comprovar as alegações que podem ou não corresponder verdadeiramente ao que se passou e deu início à formação do processo". Nesse sentido, Prova permite buscar alcançar a verdade dos fatos, mas a mesma nunca refletirá a verdade real, pois é improvável reproduzir de forma completa os fatos pretéritos em torno dos quais orbita a lide. Assim, é possível se chegar a quais foram ou são provavelmente os fatos (ALMEIDA; FARIA, 2015, p. 66).

Destarte, ainda que os meios de prova em espécie em direito admitidos estejam elencados no atual CPC, não se trata de um rol taxativo, pois outros meios de provas são admitidos, desde que não sejam contrários ao sistema normativo jurídico brasileiro, conforme previsto no artigo 369 do CPC *“As partes têm o direito de*

empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código" (BRASIL, 2015). Na busca de se confirmar as afirmações dos fatos alegados, os meios de prova são as ferramentas utilizadas pelas partes em uma demanda. Somente serão admitidos como provas válidas os meios legais e legítimos, assim considerados aqueles que contam com previsão legal e ainda os que não são proibidos por lei. Nesse sentido, alude-se prova como um direito fundamental, ainda que a prova não seja colocada como um dever, pois isso implicaria um direito de outra pessoa, ela pode ser considerada um encargo, já que a parte apresentará elementos com o intuito de comprovar suas afirmações, logo, sua aplicação é direito incondicional da parte em conflito.

2.3 DOCUMENTO ELETRÔNICO COMO MEIO DE PROVA DIGITAL NA ATUALIDADE

Segundo Marcacini (2006) documento eletrônico como meio de prova digital é manifestar uma informação que os sentidos humanos podem captar através de um software específico e um computador, ou seja, o documento eletrônico espelha um fato eletrônico, que foi elaborado ou difundido por meio eletrônico, ou que esteja armazenado em um arquivo digital, podendo o mesmo constar em um banco de dados, em um sistema, e-mail, ou em outros. Como bem nos assegura Teixeira (2015), documento eletrônico como meio de prova digital é buscar instrumento eletrônico que venha a representar um ato ou fato produzido eletronicamente por meio de um suporte material.

Para Marques documento eletrônico como meio de prova digital é a tradução de uma sequência de bits, por meio de algum programa de computadores, para se ter ciência de um fato:

> DOCUMENTO ELETRÔNICO COMO MEIO DE PROVA DIGITAL permite [...] nada mais representa que uma sequência de bits que, traduzida por meio de um determinado programa de computador, seja representativa de um fato. [...] os documentos eletrônicos possuem os mesmos elementos que um documento escrito em suporte de papel, contendo, entretanto, os seguintes aspectos: a) constam em suporte material (disquete, circuitos, chips de memória, redes); b) contêm uma mensagem, em que está escrita em linguagem convencional de dígitos binários ou bits, entidades magnéticas que os sentidos humanos não podem perceber diretamente; c) estão escritos em um idioma ou código determinado; d) podem ser atribuídos a uma pessoa determinada com a qualidade de autor, mediante uma assinatura digital ou chave eletrônica" (MARQUES, 2011, p. 127).

Conforme descrito anteriormente, documento eletrônico como meio de prova digital é aplicado para buscar a validade jurídica de um fato criado, transmitido ou armazenado em meio eletrônico, pois o conhecimento desse fato não pode de logo ser representado sem a utilização de um outro tipo de objeto apto a permitir a sua leitura. Evidentemente a aplicação pode ser utilizada para atender requisitos como a autenticidade, a integridade e perenidade do conteúdo criado, transmitido e armazenado eletronicamente, garantindo assim a força probante ao documento eletrônico como meio de prova.

Atualmente, várias pessoas utilizam um simples “prints de tela” como forma de comprovar a veracidade de fatos alegados em meio digital, no entanto, esse espelhamento da tela, não passa apenas de frágeis imagens, sujeitas a fraudes e manipulação. Pois para coletarmos uma prova digital, faz-se necessário que estejam presentes a integridade e autenticidade do documento eletrônico, pois a prova plena não pode ter sofrido alteração, deve representar o fato com rigor e de forma legítima, garantindo a veracidade de sua fonte.

Há em algumas áreas do direito uma discussão maior sobre a legalidade das provas (licitude) e pouco se aprofunda sobre a autenticidade (se corresponde à realidade). De acordo com Delmanto (2017), existe uma confusão na maneira de tratar provas documentais (obtidas a partir de documentos formais) e provas não documentais (obtidas da realidade concreta). Ambos são completamente diferentes no que se refere à autenticidade. Enquanto a prova documental tem seu embasamento de autenticidade nos processos, regulamentos e outorgas. A prova não documental obtida na realidade tem sua autenticidade fundamentada por métodos técnico científicos de coleta e preservação de provas.

Cita-se, como exemplo, a ata notarial, um meio de prova específico que conforme artigo 384 do CPC está apta a atestar ou documentar “*A existência e o modo de existir de algum fato”* (BRASIL, 2015), como supostamente verdadeiro, por ter sido lavrada por um tabelião, a confusão entre provas documentais e provas não documentais, gera a confiança sem fundamento colocada na mera fé pública de um tabelião ao "autenticar" uma prova digital.

Neste caso, como é possível se dá confiança na autenticidade à uma prova obtida a partir da realidade sem o uso de métodos técnicos adequados para tal, pois o tabelião, no caso das provas digitais, apenas descreve em um documento público o

que sua análise lhe permitiu observar, sem utilizar elementos técnicos que garantam a autenticidade e a veracidade da prova, ou seja, sem uma análise dos metadados da imagem de forma a verificar se houve adulteração.

Ainda para Marques:

> Portanto, o documento eletrônico ou o ciberdocumento é enquadrado na categoria dos documentos indiretamente representados, pois não há dele uma percepção sensorial imediata. O conhecimento de declaração representada no documento depende de recurso eletrônico, ou seja, o efeito representativo dar-se-á somente após a utilização de um outro tipo de objeto apto a permitir a sua leitura, [...]. Desta forma, verifica-se que, ontologicamente, não existe uma diferença entre a noção tradicional de documento e a nova noção de documento eletrônico, porque o ciberdocumento também será o meio real de representação de um fato, não sendo, apenas, de forma gráfica (MARQUES, 2011, p. 129,130).

Nesse sentido, documento eletrônico como meio de prova digital possui os mesmos elementos de um documento escrito, no entanto, por se tratar de fato ocorrido em ambiente digital, sua autoria é identificada a partir da assinatura digital, e em virtude de incidirem em suporte material como chips de memória, redes e outros, existe a necessidade de decodificar essa informação para um meio que seja possível ser entendido pelos sentidos humanos.

Logo, é importante compreender que existe a possiblidade de adulteração dos dados constantes no documento eletrônico, e com vistas a garantir a validade e veracidade da prova digital, faz-se necessário o uso de ferramenta que permita a coleta desses metadados com vista a integridade e autenticidade do documento eletrônico. Nesse sentido, o documento eletrônico como meio de prova digital é de grande importância para demonstrar a ocorrência ou veracidade dos fatos alegados, desde que esse documento seja coletado de forma a atender os requisitos como da autenticidade, integridade e perenidade do conteúdo.

3 CADEIA DE CUSTÓDIA E A COLETA DE PROVAS DIGITAIS NA ATUALIDADE

Ao tratar das provas digitais na atualidade, prova não documental obtida da realidade concreta, nos deparamos com a necessidade, durante a sua coleta, do cumprimento da cadeia de custódia, como garantia da autenticidade dessa prova, já que deve ser aferida através de métodos técnicos científicos.

3.1 DA CADEIA DE CUSTÓDIA

Na doutrina brasileira, a cadeia de custódia pode ser compreendida como o procedimento que visa aferir a autenticidade da prova, como forma de garantir que os indícios coletados no incício da investigação correspondam ao que será apreciado em juízo, conceituando-a como:

> (...) 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. Funciona, pois, como a documentação formal de um procedimento destinado a manter e documentar a história cronológica de uma evidência, evitando-se, assim, eventuais interferências internas e externas capazes de colocar em dúvida o resultado da atividade probatória, assegurando, assim, o rastreamento da evidência desde o local do crime até o Tribunal (LIMA, 2020, p. 718).

Em sentido amplo, pode ser definida como a série de etapas ou procedimentos que devem ser realizados para garantir e assegurar que a prova colhida ou envolvida em um fato existe ou permanece em boas condições até o momento do julgamento (PRADO, 2019).

Consiste em assegurar a idoneidade do material coletado, dirimindo dúvidas quanto à sua origem e o caminho percorrido, desde o início da coleta, quem recolheu, quem entregou, quem analisou, a quem os resultados foram entregues, até seu envio ao tribunal, visando demosntrar que o mesmo objeto apresentado em juízo é o mesmo apreendido na data do fato (LIMA, 2020). O pessoal envolvido na cadeia de custódia deve estar ciente de que, se não fizer seu trabalho adequadamente, corre-se o risco de quebrar qualquer vínculo e atrapalhar todo um processo que terá consequências legais posteriores para a correta aplicação da justiça (EDINGER, 2016).

O objetivo da cadeia de custódia não é viciar o tratamento de provas e indícios, e sim evitar alterações, substituições, perda ou destruição de provas, preservando-as no estado em que foram encontradas, de forma que sua relação com os fatos que são investigados sem a dúvida (LOPES et al, 2006).

> A cadeia de custódia visa assegurar a idoneidade dos objetos e bens apreendidos, de modo a evitar qualquer tipo de dúvida quanto à sua origem e caminho percorrido durante a investigação criminal e o subsequente processo criminal. Em outras palavras, se a acusação pretende apresentar evidências físicas em juízo (v.g., arma do crime), deve estar disposta a mostrar que o objeto apresentado é o mesmo que foi apreendido na data dos fatos (LIMA, 2020, p.720).

O processo de construção da Cadeia de Custódia deve ser conservado desde o instante em que as provas são encontradas, analisadas pelo Laboratório Central de Criminalística e armazenadas até a finalização do Julgamento Oral e Público. Ao não realizar uma correta cadeia de custódia, as evidências ficam contaminadas, terceiros podem ser envolvidos e pode ser criada a impunidade (LOPES et al, 2006).

No sistema normativo jurídico brasileiro, em regra, prevalece o impedimento do uso da prova ilícita, da mesma forma, são admitidos todos os meios probatórios, desde que legal ou moralmente legítimos, neste sentido, é válida a prova adquirida por meio eletrônico (PRADO, 2019).

Como os supostos direitos que constam do litígio têm origem em fatos, eles precisam ser demonstrados, ou seja, para que a sentença declare o direito, o juiz precisa certificar a veracidade do fato alegado, e essa demonstração se dá por meio de provas (MONTEIRO, 1912). Assim, ao requerer a tutela jurisdicional, o cidadão tem que oferecer as provas, até então existentes, para fundamentar o seu pedido, bem como postular a produção de outras provas cabíveis. Isso se faz necessário porque o magistrado, para declarar a existência do direito de punir determinado indivíduo, precisa conhecer os fatos e estar convencido de sua ocorrência e autoria (PRADO, 2019).

O exame da veracidade dos fatos relatados é feita pelo juiz, por meio das provas trazidas ao processo (MONTEIRO, 1912, p.93). A princípio "todos os meios legais, bem como os moralmente legítimos", ainda que não especificados em lei, "são capazes de provar a veracidade dos fatos, em que se baseia a ação ou defesa"(PRADO, 2019). Para limitar o princípio da liberdade de prova e evitar abusos,

a Carta Magna de 1988 estabeleceu que "é inadmissível no processo a prova obtida por meios ilícitos" (inciso LVI, do art. 5º) (BRASIL, 1988).

Há pelo menos três correntes doutrinárias sobre a admissibilidade da prova ilícita: a "teoria da inadmissibilidade absoluta", que entendem, como premissa, que a vedação constitucional não admiti exceção ou relativização; a “teoria da admissibilidade processual da prova Ilícita” admitindo as provas ilegais desde que não vedadas pelas disposições processuais; e a “teoria da admissibilidade relativa” que, à luz do princípio da proporcionalidade, acolhe a tese da relativização da proibição constitucional da prova ilícita (LOPES JUNIOR, 2019, p. 476).

Com o advento da Carta Magna brasileira de 1988 e a previsão de que “a prova obtida por meios ilícitos é inadmissível no processo” a inadmissibilidade da prova ilícita conquistou vários seguidores, encontrando algum abrigo na jurisprudência (LOPES JUNIOR, 2019, p. 475). Com o passar do tempo, principalmente devido ao entendimento e amadurecimento normativo dos direitos humanos, a teoria da inadmissibilidade absoluta das provas ilícitas perdeu força diante do esmaecimento de princípios relacionados à prática dos direitos fundamentais, como a proporcionalidade, ponderação e adequação (EDINGER, 2016).

Atualmente a teoria predominante é a do argumento de relativizar a proibição de provas ilícitas devido à comparação de princípios constitucionais em aparente conflito, prescindindo a ponderação que é necessária em virtude da complexidade que envolve cada caso na sua particularidade. A teoria da inadmissibilidade da prova ilícita, não admite qualquer tipo de prova ilícita, independentemente da relevância do direito em discussão, sempre rejeitando provas ilícitas, provas ilegítimas e derivadas. “Tal teoria encontra eco, principalmente, nos casos em que na obtenção da prova (ilícita) são violados direitos constitucionalmente assegurados”(LOPES JUNIOR, 2019, p. 476).

Os defensores desta tese, alegam que as provas obtidas por meios ilícitos devem ser eliminadas do processo, por mais elevados e relevantes que sejam os fatos comprovados. Eles compartilham os mesmos critérios, citando a teoria dos frutos da árvore envenenada como fundamento para a inadmissibilidade de provas ilícitas em qualquer situação, não importando, para a análise, a relevância da a lei em debate. Nessa linha, a prova ilícita deve ser sempre rejeitada porque confronta, além do direito material, o processual, os princípios e garantias constitucionalmente assegurados (LIMA, 2020).

> Portanto, pode-se dizer que, no ordenamento pátrio, por mais relevantes que sejam os fatos apurados por meio de provas obtidas por meios ilícitos, estas não podem ser admitidas no processo. Se, mesmo assim, uma prova ilícita for juntada ao processo, surge o direito de exclusão, a ser materializado através do desentranhamento da referida prova dos autos (LIMA, 2020, p.688).

Essencialmente, a teoria da inadmissibilidade absoluta da prova ilícita visa impedir que as partes que desejam provar suas objeções por meio da prova ilícita, não às faça, com vista a ponderar a busca irrestrita pela verdade dos fatos e o respeito aos direitos fundamentais, o que ensejaria a ilegalidade da prova e por indução a sua inadmissibilidade:

> A discussão em torno da (in)admissibilidade das provas obtidas por meios ilícitos ou ilegítimos em determinando ordenamento jurídico está diretamente relacionada à opção entre a busca ilimitada da verdade, dando-se preponderância ao interesse público na persecução penal, e o respeito aos direitos e garantias fundamentais, dentro de uma visão ética do processo, ainda que em prejuízo à apuração da verdade.
> (...)
> Com a Constituição Federal de 1988, entre os direitos e garantias individuais, estabeleceu-se a inadmissibilidade das provas obtidas por meios ilícitos (art. 5º, LVI). Logo, a sanção processual cominada para a ilicitude da prova é a sua inadmissibilidade. Não se trata de nulidade da prova, mas de sua não aceitação nos autos do processo (LIMA, 2020, p.687-688).

Ao analisar em profundidade a relativização da ilegalidade da prova obtida em violação ao direito material em face do princípio da proporcionalidade (EDINGER, 2016), o ordenamento jurídico brasileiro “não contempla expressamente dito”, esclarecendo que é preciso analisar com muita cautela a aplicação de um princípio não previsto na Carta Magna brasileira de 1988, como o da proporcionalidade. Segundo Aury Lopes Júnior:

> Para os seguidores dessa corrente, a prova ilícita, em certos casos, tendo em vista a relevância do interesse público a ser preservado e protegido, poderia ser admitida. Abranda a proibição para admitir a prova ilícita, em casos excepcionais e graves, quando a obtenção e a admissão forem consideradas a única forma possível e razoável para proteger a outros valores fundamentais. A intenção é evitar aqueles resultados repugnantes e flagrantemente injustos (LOPES JUNIOR, 2019, p. 476).

Neste diapasão, reconhece-se a possibilidade de se admitir a relativização de provas ilícitas por derivação, mas apenas quando não for evidenciado o nexo de causalidade entre uma e outra, ou quando as derivações puderem ser obtidas por fonte independente da primeira (LOPES JUNIOR, 2019, p. 480).

Dessa forma, ficou estabelecido que as provas ilícitas aludidas conforme a Constituição Federal brasileira de 1988 são aquelas obtidas em violação às normas constitucionais; “prova ilícita: é aquela que viola regra de direito material ou a Constituição no momento da sua coleta, anterior ou concomitante ao processo, mas sempre exterior a este” (LOPES JUNIOR, 2019, p. 473). Assim, para poder comparar uma relativização na ilegalidade da prova, mesmo com base no não absolutismo dos princípios constitucionais, seria necessário, em primeiro lugar, alterar o texto constitucional para que a ponderação dos princípios é realizado por meio de critérios de aplicação determinados por lei e não apenas pelo aspecto avaliativo, sob pena de entrar em um temível campo de subjetividade (EDINGER, 2016).

O legislador constituinte de 1988, sustenta que quando quis, isentou a regra, e o fez expressamente, como no artigo 5º, incisos XI e XII. Portanto, além daqueles casos expressos e exaustivos não seria possível relativizar a ilegalidade da prova processual, independentemente da matéria *sub judice* (EDINGER, 2016). Para justificar sua tese, menciona-se uma jurisprudência de matéria penal do Supremo Tribunal Federal, no relatório do Ministro Carlos Velloso, que segundo sua interpretação, rejeitaria o uso de provas ilícitas e confirmaria o uso de provas lícitas recorrentes de conduta que, via de regra, seriam ilegais, mas que ganham personalidade jurídica quando produzidos pelo próprio acusado para sua defesa (PRADO, 2019).

Em suma, em razão da teoria da inadmissibilidade da prova ilícita, a prova ilícita não pode ser utilizada, principalmente porque está previsto expressamente no inciso LVI, do artigo 5º, da Constituição Federal de 1988, bem como a doutrina e a jurisprudência não podem inserir exceções interpretativas ao referido inciso (LIMA, 2020, p. 685-687), por além das restrições dos incisos XI e XII, do mesmo artigo, sob pena de colocar em risco a segurança jurídica e afrontar o estado democrático de direito.

Dentro desse cenário, ressalta-se que a prova digital, para que seja considerada válida, necessita ter sido coletada eletronicamente, resguardando o cumprimento da cadeia de custódia, de forma a permitir que as partes e os juízes possam periciar cronologicamente a marcha da produção da prova, desde a sua identificação, o local do meio digital, a sua coleta e a extração do resultado, com o propósito de confirmar a idoneidade e autenticidade como meio probatório (PRADO,

2019). Assim, ressalta-se que perante a Lei n. º 13.964/2019, existe a importância da utilização da cadeia de custódia do processo penal em dados digitais.

3.2 DA CADEIA DE CUSTÓDIA DAS PROVAS DIGITAIS

A cadeia de custódia digital é o procedimento que permite conhecer de forma inequívoca a identidade, integridade e autenticidade dos vestígios ou sinais digitais relacionados a um ato criminoso, desde o momento em que são encontrados até serem fornecidos ao processo judicial como meio de prova (PRADO, 2019).

A importância de preservar corretamente a cadeia de custódia digital, devido às características especiais da prova digital, está no fato de poder garantir seu uso como prova. “(..) a cadeia de custódia no direito, ultrapassa fronteiras e assume um significado muito mais amplo com os elementos imateriais como evidência, assumindo a possibilidade de fonte de prova dos documentos digitais” (FLORES, 2020, p. 37).

O objetivo da cadeia de custódia é garantir a identidade exata do que é apreendido e analisado. Portanto, a cadeia de custódia digital tem um valor instrumental, pois serve para garantir que o que é analisado e apresentado em juízo como prova, é o mesmo que a prova digital coletada (FLORES, 2016).

A cadeia de custódia digital garante a fidedignidade da prova digital fornecida no julgamento e a defesa adequada através do perito informático correspondente (LUZ; FLORES, 2018). É imprescindível dentro do procedimento pericial informático/tecnológico, garantir sua autenticidade e integridade, pois pode ser facilmente manipulado (NETO; SANTOS, 2020).

Seguir o processo correto da cadeia de custódia digital evita a contaminação das evidências. Dentro da preservação de elementos e dispositivos digitais, as chaves HASH são especialmente importantes, que é uma impressão digital usada para identificar o conteúdo de um arquivo dentro de uma sequência de caracteres. Ao contrário dos meios tradicionais de evidência, a evidência digital tem como principais características ser:

- Intangível: A evidência digital é intangível, não podendo ser apreciada diretamente pelos sentidos, mas por meio de complexos processos computacionais (NETO; SANTOS, 2020).

- Replicável: A prova é em formato digital, podendo ser copiada ou replicada quantas vezes desejar. Isso levanta o problema de distinguir a prova original da cópia, porém, se puder ser provado inequivocamente que ambas são exatas, pouco a pouco, a força probatória é a mesma (NETO; SANTOS, 2020).
- Volátil: A prova digital é inconstante devido à sua própria natureza intangível e está especialmente sujeita à possibilidade de modificação ou alteração, o que acrescenta complexidade especial para que uma prova digital adquira capacidade probatória (NETO; SANTOS, 2020).
- Apagável: A prova digital pode ser facilmente destruída, não sendo necessária em todos os casos a destruição do suporte digital que a contém (NETO; SANTOS, 2020).
- Parcial: Às vezes, a prova digital é composta por vários arquivos de computador, espalhados por diferentes meios e locais digitais, como um sistema de informação na nuvem, o que agrega ainda mais complexidade à sua apreensão e preservação (NETO; SANTOS, 2020).

Dentro de qualquer regulamentação legal de qualquer ordem jurisdicional, a prova digital passa por três fases dentro do processo de cadeia de custódia digital:

- **A primeira fase** consiste na obtenção dos dados produzidos, armazenados ou transmitidos através do acesso às fontes da prova digital antes da sua incorporação no processo, está relacionada ao **princípio do Isolamento** da cadeia de custódia. Nesta fase, tanto as partes quanto a autoridade pública devem acessar os dados de forma lícita, ou seja, sem violar direitos fundamentais ou qualquer outra regulamentação aplicável (DOS SANTOS LUZ, 2018).
- **A segunda fase** está relacionada aos **princípios do Reconhecimento, Fixação e Coleta** da cadeia de custódia, consiste na incorporação no processo dos dados relevantes para a acreditação dos fatos, com três tipos de requisitos: Relevância e necessidade de prova digital sobre o fato controverso objeto do caso; Legalidade, entendida como respeito aos direitos fundamentais e normas aplicáveis durante a prática da prova; Cumprimento dos requisitos das leis processuais, ou seja, que a prova digital acesse o processo de acordo com o procedimento probatório contemplado para a restituição respectiva ordem jurisdicional para exercer validamente o direito à prova (DOS SANTOS LUZ, 2018).

- **A terceira fase** consiste na avaliação dos dados pelo órgão julgador. Está relacionada ao **princípio do Acondicionamento** da cadeia de custódia**.** Respeitadas as duas fases anteriores, a prova digital terá valor probatório e poderá ser apreciada. A obtenção de informações (elementos de convicção) constitui uma das facetas mais importantes dentro de uma investigação criminal, aspecto que exige dos investigadores/peritos responsáveis pela recolha, preservação, análise e apresentação de provas digitais um trabalho eficaz que garanta a autenticidade e integridade das referidas provas, a fim de assegurar que sejam levadas em consideração em um processo judicial (DOS SANTOS LUZ, 2018).

Em suma, a cadeia de custódia garante a confiabilidade da prova digital fornecida em um julgamento. No entanto, como mencionado, a manipulação da prova digital é fácil, sendo a cadeia de custódia necessária para preservar adequadamente a autenticidade e integridade das provas digitais (LUZ; FLORES, 2018). A quebra da cadeia de custódia digital favorece a absolvição de cibercriminosos e outros criminosos que deixam provas em dispositivos eletrônicos, como aconteceu com o caso Anonymous no Tribunal Criminal número 3 de Gijón. Uma das chaves para a absolvição foi a quebra da cadeia de custódia e o recolhimento de peças sem a devida custódia policial e judicial, bem como a inadequada preservação das provas até o julgamento, levando ao entendimento de que essas provas poderiam ter sido manipuladas no decorrer deste processo:

> Na seção sobre os fundamentos jurídicos da sentença, contra a qual cabe recurso, o juiz admite que ocorreu **“a violação do direito a um processo com as devidas garantias”, uma vez que houve quebra na cadeia de custódia dos dispositivos apreendido do acusado após sua prisão. “No presente caso, a confusão e contradição observadas quanto à adoção de garantias suficientes para preservar a identidade e integridade dos bens apreendidos dos três réus e quanto à sua eventual manipulação ou contaminação ultrapassa a mera suspeita e vem à tona. cadeia de custódia", reconhece a sentença.**
> Assim, dispensadas as provas relativas aos aparelhos apreendidos e os laudos periciais a eles relacionados, o magistrado concentra-se na análise das provas documentais e testemunhais e conclui que não foram comprovados os crimes de que foram acusados. “Após a apreciação direta em plenário das provas testemunhais, do perito em extremos não relacionados aos dispositivos apreendidos, e das declarações dos acusados em relação ao documentário fornecido, conclui-se que não ficou provado que os acusados pertencia ao coletivo Anonymous", conclui o magistrado (EL COMERCIO, 2016, grifos autorais).

A perícia informática neste caso mostrou que os códigos HASH do material apreendido ao arguido não coincidiam com os que tinham sido obtidos pela polícia e

registados nos autos durante a intervenção. Portanto, a prova foi declarada contaminada, inválida e não confiável, pois não havia certeza absoluta de preservação e autenticidade da prova digital. Por outro lado, investigar e processar crimes cibernéticos costuma ser mais complexo do que investigar e processar crimes "físicos". Os crimes cibernéticos proporcionam uma sensação de impunidade ao cibercriminoso devido ao anonimato que a Internet oferece (MEDEIROS; UGALDE, 2020).

A isso se soma o fato de que é muito difícil obter, coletar e preservar provas digitais devido às suas características especiais, como vimos, portanto, seguir uma correta cadeia de custódia garantirá que as provas obtidas possam ser usadas em um processo judicial (NETO; SANTOS, 2020).

Refletindo sobre a utilização da prova digital no ordenamento jurídico brasileiro, mencionamos o Projeto de Lei 4939/2020 que está em tramitação na Câmara dos Deputados redigido por Hugo Leal do PSD-RJ que dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências. A aprovação dessa lei é de suma importância para basilar critérios e a forma de coleta das provas digitais, servido de norte para que estas provas possam ser usadas de forma válida em um processo criminal (CÂMARA DOS DEPUTADOS, 2020).

Neste diapasão, a aprovação do Projeto de Lei 4939/20 que busca estabelecer os princípios e regras para a obtenção e a admissibilidade de provas digitais durante a investigação, bem como no processo criminal, é de fundamental relevância, tendo em vista que as provas em meio eletrônico são uma realidade tanto nos processos civis quanto nos processos criminais, destarte, com a tecnologia cada vez mais presente no cotidiano da sociedade, as provas digitais irão prevalecer cada vez mais na instrução processual.

3.3 FRAGILIDADE DA COLETA DAS PROVAS DIGITAIS EM RELAÇÃO A AUTENTICIDADE PROBATÓRIA

Dentro dos princípios que regem o julgamento acusatório, dois são de grande relevância para a forma de proceder em matéria de prova: o imediatismo e o contraditório (LIMA, 2020). A primeira exige que as provas (salvo exceções) sejam

divulgadas na audiência, ou seja, na presença do juiz para que ele a perceba diretamente. Consequentemente, para ter valor, qualquer elemento fornecido para fins de prova deve ser avaliado na presença do magistrado (LIMA, 2020).

De tal forma, que em virtude do princípio do imediatismo, no caso por exemplo de fotografias e outros meios visuais de prova, produzidos previamente à audiência, devem ser descritos e corroborados perante o juiz por quem as produziu para que possam atestar a sua autenticidade e procedência; mas também dos elementos técnicos que intervieram na sua elaboração e as consequências que estes pormenores acarretam (NETO; SANTOS, 2020).

Em outras palavras, o objeto, a fotografia por exemplo, por si só não é suficiente; isso parece óbvio quando se trata da arma do crime; no entanto, quando se trata de elementos visuais (como fotografias) pode-se supor que eles são objetivos e, portanto, "falam por si", presumir-se-ia que não são necessários mais requisitos do que apresentá-los para demonstrar seu conteúdo, o que não é o caso, como veremos ao destacar os elementos semióticos da imagem em geral e das fotografias de identidade em particular; mesmo que, em grande parte dos casos, fazem parte de arquivos compostos por fotografias anteriores aos fatos, de modo que não se sabe que os detalhes de sua produção devem ser lembrados no momento da prova apresentada (NETO; SANTOS, 2020).

Além disso, como se sabe, um número significativo de sujeitos são presos como prováveis autores com base em arquivos de identidade fotográfica, que são formados ao longo do tempo e, portanto, pode advir equívocos e falhas da mente humana em relação as imagens, por estas não serem confiáveis para a identificação de um indivíduo (ROCHA; TELES, 2021).

Como exemplo podemos citar o recente caso, que foi manchete do Fantástico (17/04/2022), referente a decisão do Superior Tribunal de Justiça, nos autos do HC nº 705770/RJ (2021/0360804-9), que tinha como paciente o sr. Silvio José da Silva Marques (PRESO), conhecido como Silvio Pantera, lutador de MMA, que foi condenado e preso por seis anos por um crime que não cometeu, em virtude do reconhecimento por meio de fotografia e a não apreciação de provas digitais que demonstravam que o réu no momento do crime estava em uma academia, conforme poderia ter sido comprovado através da digital na roleta de entrada da academia, prova que foi juntada aos autos pelo advogado de defesa, mas não foi verificada. O

STJ absolveu o Sr. Silvio José da Silva Marques de todas as acusações (BRASIL, 2022a).

A prisão, seguir-se-á ainda procedimento em que ele poderá ser posto em liberdade, como ocorreu no caso acima exemplificado, no entanto os danos já terão sido causados pelo simples fato de estar preso. Em virtude do segundo princípio, o do contraditório, o julgamento deixa de se apresentar como busca da verdade pelo juiz. Nesse sistema, cada parte apresenta sua teoria do caso, a versão do ocorrido que permite colocar o comportamento da parte que representa sob sua melhor luz, ou seja, “partes em posições antagônicas, uma delas obrigatoriamente em posição de defesa (ampla defesa), havendo a necessidade de que cada uma tenha o direito de se contrapor aos atos e termos da parte contrária (contraditório) ”. (LIMA, 2020, p. 58).

Em outras palavras, duas versões opostas do que aconteceu devem se enfrentar; A decisão do juiz deve ser gerada a partir dessas duas visões opostas. A partir disso podemos entender o interesse de mostrar até que ponto a falta de univocidade das imagens apresentadas como evidência deve ser levada em conta, pois, a preservação de uma prova digital busca “à proteção de sua integridade para garantia de sua utilidade e validade probatória” (NETO; SANTOS, 2020, p.10).

O uso de imagens é controverso dentro do ordenamento jurídico brasileiro, inclusive sendo proibido pelo Superior Tribunal Federal como prova. De acordo com o STF as capturas de telas de *Whatsapp* não são provas válidas, haja vista que as mensagens do aplicativo podem ser manipuladas, com a supressão de mensagens que podem alterar o contexto de uma conversa. Além do mais, as imagens podem fazer parte de um contexto antigo e não se referir exatamente sobre a causa de uma ação específica (LUZ; FLORES, 2018). Dessa forma, fica claro que o uso de prints de conversa de *Whatsapp* estão vedadas como provas digitais. Um exemplo de decisão que proibiu o uso de imagens de *Whatsapp* como prova refere-se a um caso julgado pela 6ª turma do Superior Tribunal de Justiça, no processo RHC 133.430/PE. Esta ação se refere a uma acusação de crime de corrupção passiva contra três pessoas. Nesse julgado, a defesa apresentou a capturas de telas com conversas no aplicativo *Whatsapp*, que comprometiam os réus. A entrega desses prints gerou grande inquietação da defesa, que disse que os réus estavam sofrendo constrangimento ilegal, pois não seria possível e de forma factível provar a autenticidade dessas provas, que foi deferido pelo juiz e essa prova foi exclusa dos autos (ACMINAS, 2022).

Semelhante decisão foi proferida pelo STJ nos autos do Habeas Corpus nº 718849 – SP, como pode ser verificado na ementa abaixo:

> HABEAS CORPUS Nº 718849 - SP (2022/0015519-6) DECISÃO Cuida-se de habeas corpus com pedido liminar impetrado em favor de LENON CESAR DE OLIVEIRA em que se aponta como autoridade coatora o TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO (Apelação Criminal n. 0001544-38.2016.8.26.0042). O paciente foi condenado às penas de 1 ano, 6 meses e 20 dias de reclusão no regime semiaberto e de 14 dias-multa, como incurso no art. 140, § 3º, c/c o art. 141, inciso III, ambos do Código Penal. **O impetrante sustenta que o édito repressivo estaria lastreado em prova inválida, consistente no espelhamento de conversas por meio do aplicativo WhatsApp. Afirma que a ferramenta permite o envio de novas mensagens e a exclusão de mensagens antigas ou recentes, tenham elas sido enviadas pelo usuário ou recebidas de algum contato, sem deixar vestígios no aplicativo ou no computador, razão pela qual a captura das telas de conversas constituiria prova nula.**
> [...] **A propósito, não se desincumbiu a Defesa de comprovar a imaginária versão de que algumas mensagens foram apagadas com a intenção de editar o print**, ônus que lhe incumbia (artigo 156 do Código de Processo Penal), até porque tal prova seria de fácil produção, bastando exibir texto de celular do réu com o verdadeiro contexto ou do aparelho de qualquer um dos vinte e cinco integrantes do grupo de WhatsApp. **Como observou o magistrado, "também é importante consignar que a própria defesa do réu apresentou desistência quanto ao prosseguimento do incidente de falsidade instaurado para apurar eventual adulteração da imagem, o que, aliada aos outros elementos (como a versão da testemunha Thiago de que apresentou a mesma imagem por intermédio de seu aparelho à vítima), a torna totalmente verdadeira" (fls. 194/195)**.
> [...] Ante o exposto, indefiro o pedido de liminar. Solicitem-se informações ao Tribunal de origem, que deverão ser prestadas preferencialmente por malote digital e com senha de acesso para consulta ao processo. Dê-se vista ao Ministério Público Federal. Publique-se. Intimem-se. Brasília, 25 de janeiro de 2022. MINISTRO JORGE MUSSI Vice-Presidente, no exercício da Presidência (BRASIL, 2022b, grifo nosso)

Como foi possível observar na decisão acima, o juiz entendeu que o *Whatsapp* permite o envio de novas mensagens e a exclusão de mensagens antigas ou recentes, tenham elas sido enviadas pelo usuário ou recebidas de algum contato, sem deixar vestígios no aplicativo ou no computador, razão pela qual a captura das telas de conversas constituiria prova nula. Como pode-se perquirir existem muitos desafios para tornar as provas digitais meios de se tornarem provas em um processo (NETO; SANTOS, 2020).

Prova Digital ou Prova Eletrônica é qualquer valor probatório de informação acondicionada ou transmitida em formato eletrônico, de forma que parte ou toda ela possa ser utilizada em juízo (CASEY, 2011). Previamente, para que a prova digital seja aceita, o tribunal determinará se a mesma é pertinente, autêntica, se é boato e se é aceitável uma cópia ou se é necessário o original (CASEY, 2011). O problema

da aceitação da prova digital em juízo é que esta evidência digital pode ser facilmente manipulada. E devido a uma falta global de regulamentação em questões tecnológicas, é tecnicamente possível falsificar tudo, desde SMS, bate-papos no whastapp, e-mails ou postagens em redes sociais. É o que ocorre, por exemplo, com a Ata Notarial ela é aceita como prova se for física, porém como prova digital não possui mecanismo que preserve o documento eletrônico, pois não é possível aferir sua autenticidade (GONÇALVES, 2018):

> A ata notarial não resguarda a proteção do documento digital nem na sua formação nem após. Não há controles de verificação de integridade nem de autenticidade. Mesmo assim, o artigo 405 do CPC determina que o "documento público faz prova não só da sua formação, mas também dos fatos que o escrivão, o chefe de secretaria, o tabelião ou o servidor declarar que ocorreram em sua presença. (GONÇALVES, 2018)

Estes elementos acima elencados são, sem dúvida, amplamente utilizados na acusação em inúmeros processos judiciais em todas as ordens jurisdicionais, e se não houver impugnação da referida prova através do correspondente laudo pericial informatizado, pressupõe-se a aceitação tácita da autenticidade da prova. Em referência ao nosso país, a publicação nas redes sociais de informações de terceiros é especialmente problemática, devido à volatilidade das evidências (NETO; SANTOS, 2020).

Uma publicação que passa a ser deletada uma ou duas horas depois, foi vista e compartilhada por milhares de pessoas, o que claramente põe em risco os direitos fundamentais dos cidadãos e afeta gravemente o normal exercício da justiça, não podemos deixar de reconhecer que a prova digital é de grande importância no processo judicial, independentemente do ramo do direito que se apresente, seja civil, criminal, pois a prova digital em virtude dos conteúdos virtuais acondicionados em aparelhos tecnológicos, vem influenciado e ganhando relevância no dia a dia da sociedade, bem como na busca por esclarecimentos das provas na área penal e processual penal. (NETO; SANTOS, 2020).

Finalmente, como resultado de tudo o que foi dito acima, podemos começar a fazer uma hipótese e ao final, entendemos o que realmente aconteceu, mas o que não podemos saber é o tempo que isso pode levar, ficando à mercê de várias lacunas, não apenas legal, mas também informatizada, pois não existe uma regulação global do ciberespaço. Mas, sem dúvida, o aqui levantado é o caminho para uma conclusão

bem-sucedida, basta invocar plenamente as políticas estatais urgentes sobre essas questões que já fazem parte do nosso cotidiano, em busca de atender o número cada vez maior de demandas referentes aos crimes digitais, pois quando um crime é cometido os danos causados podem ser irreversíveis (NETO; SANTOS, 2020).

É por isso que através da prova digital, podemos evidenciar um ato criminoso ou não, de acordo com o registro digital coletado, o que nos leva à posse da verdade, para isso devemos obter essa prova através da cadeia de custódia digital, “pela qual se assegura que esses documentos são os mesmos desde o início, não sofreram nenhum processo de alteração e, portanto, são autênticos” (FLORES, 2016, slide 15). O que deve ser exigido por nossas leis para obter a verdade do ocorrido, e é aí que reside o grande problema que é a dificuldade na resolução de crimes em ambientes digitais, sendo necessária a regulamentação em relação a cadeia de custódia das provas digitais de forma a abranger qualquer fonte de prova de natureza real, ou seja, contemplem os elementos ‘imateriais’, como os registros eletrônicos, e-mails, fotografias digitais e etc. (MACHADO, 2020).

Poderemos alcançar e contar com, num curto espaço de tempo, os instrumentos processuais adequados para combater os problemas criminais informáticos do século XXI com a legislação do século XXI, que é o grande desafio estratégico que nos espera enquanto país e enquanto sociedade, para poder entrar com sucesso nesta nova era tecnológica, nunca vista na história do mundo e da humanidade.

Neste diapasão, tratando-se a prova digital de uma prova não documental, e que deve ser aferida através de métodos técnicos científicos, bem como diante da necessidade do preenchimento de lacunas legais, pois não existe uma regulação global do ciberespaço, vemos no cumprimento das fases da Cadeia de Custodia digital o caminho adequado na coleta dessas provas *sui generis*, na busca da garantia da sua autenticidade e integridade.

4 FERRAMENTA DE COLETA DE REGISTROS DIGITAIS PARA FINS JUDICIAIS

Neste capítulo trataremos de uma ferramenta de coleta de registros digitais utilizada para fins judiciais, buscando demonstrar que o seu funcionamento obedece às fases da cadeia de custódia na coleta de provas digitais, com fins a garantir a autenticidade e integridade dessa prova.

4.1 ETAPAS ESSENCIAIS PARA A COLETA E PRESERVAÇÃO DA PROVA DIGITAL

De acordo com a lei 13.964/2019, conhecida como o pacote anticrime, temos 05 princípios da cadeia de custódia que versam sobre as fases essenciais para a coleta e preservação de uma prova de forma confiável, sendo eles: **Reconhecimento, Isolamento, Fixação, Coleta e Acondicionamento**. Estes princípios estão presentes nas 03 (três) fases dentro do processo da cadeia de custódia digital, contextualizada no terceiro capítulo.

Considerando que o processo de coleta e preservação de uma prova digital deve cumprir as três fases da cadeia de custódia digital, neste sentido, para corroborar temos como base a Norma ABNT NBR ISO/IEC 27037:2013, que é padrão internacional, e fornece diretrizes específicas no manuseio de evidências digitais, tais como a identificação, coleta, aquisição e preservação. Esta norma tem como objetivo padronizar o tratamento dessas evidências digitais.

Vinícius Oliveira (2019) afirma que a norma ISO 27037:

> "[...] é padrão internacional para identificação, coleta, aquisição e preservação de evidências forenses digitais em todas as etapas no processo de investigação. Esta norma faz parte das 45 normas da família ISO 27000 – Gestão da Segurança da Informação. Sem dúvidas, uma das normas mais relevantes para profissionais que seguem ou pretendem seguir carreira de perito forense.
> [...] A Norma ABNT NBR ISO/IEC 27037:2013 tem por finalidade padronizar o tratamento de evidências digitais, processos esses fundamentais em uma investigação afim de preservar a integridade da evidência digital – **metodologia esta, que contribuirá para obter sua admissibilidade, força probatória e relevância em processos judiciais ou disciplinares.**
> **Esta norma assegura que os indivíduos gerenciem a evidência digital por meio de métodos práticos aceitáveis mundialmente, com o objetivo de padronizar a investigação envolvendo dispositivos digitais e/ou evidências digitais de maneira sistemática e imparcial, com o objetivo de preservar a sua integridade e autenticidade** " (OLIVEIRA, 2019, grifo nosso).

Destarte, o procedimento técnico adotado no momento da coleta e durante todo o tratamento da prova é critério com vistas a garantir sua confiabilidade em juízo, nesta perspectiva, é de suma importância a adoção das medidas previstas na norma ABNT NBR ISO/IEC 27037:2012:

> Há necessidade de emprego das regras de cadeia de custódia para fins de preservação, coleta e armazenamento da prova digital. Para tanto, em caso de busca e apreensão, apontam enquanto modelo ideal, que o perito computacional forense acompanhe a autoridade policial e seus agentes visando a coleta dos vestígios digitais dentro dos padrões estabelecidos pela norma ABNT NBR ISO/IEC 27037:2012 viabilizando a produção de prova íntegra e autêntica, o que poderá, eventualmente, viabilizar a prisão em flagrante do investigado, como, por exemplo, em crimes permanentes, cujo contexto se inserem os casos de posse ou compartilhamento por redes P2P de material pornográfico infanto-juvenil, sem riscos de prejudicar a prova da materialidade da infração.
> Salientam, ainda, a adoção da norma ABNT NBR ISO/IEC 27037:2012 em conjunto com o Procedimento Operacional padrão veiculado pela SENASP enquanto referência metodológica para fins da produção da prova pericial em dispositivos informáticos (NETO; SANTOS, 2020, p. 12).

A norma ISO 27037, estabelece que o registro da cadeia de custódia contenha no mínimo as informações referentes ao identificador único da evidência; quem acessou a evidência e o tempo e local em que isto ocorreu; quem e quando ocorreu a checagem da evidência interna e externamente nas instalações de preservação; qual o motivo da evidência ter sido verificada, ou seja, qual o propósito; a informação da autoridade relevante, quando aplicável; bem como, demais modificações impreteríveis da evidência digital, bem como o nome do indivíduo responsável pelas modificações e o fundamento para a introdução da alteração (CAPOZZI, 2019).

Em conformidade com os conceitos aplicáveis de normas internacionais da ISO 27037 e os princípios relativos a cadeia de custódia, previstos na Lei 13.964/2019, temos as 03 (três) fases essenciais para a coleta e preservação da prova digital (MUNHOZ, 2021):

1. A primeira fase é o Isolamento: Nesta etapa o objetivo é evitar a ocorrência de contaminações ou manipulações da prova durante sua coleta, seja intencional ou não, conforme o **princípio do isolamento** da cadeia de custódia digital.

2. A segunda fase é a Coleta técnica detalhada: Neste momento faz-se necessária à coleta de vários dados referentes ao fato digital, buscando possibilitar

sua perícia, bem como para sua apresentação na esfera judicial, assegurando o contraditório e ampla defesa. Esta etapa está relacionada aos princípios da cadeia de custódia digital referentes ao **reconhecimento, fixação e coleta**. Em relação as questões técnicas, busca reconhecer as informações relevantes, intentando de forma técnica e metódica, espelhar aquela realidade, com o máximo de detalhes possíveis, desde os aparentes e os não aparentes/metadados, permitindo que posteriormente o material possa ser analisado ou periciado (OLIVEIRA, 2022).

3. A terceira fase é a Preservação: Neste momento final, busca-se preservar de forma confiável a informação coletada, com o intuito de evitar alterações posteriores, bem como resguardar a identificação do emissor, está etapa está relacionada ao **princípio do acondicionamento**.

Conforme descrito pela lei e normas forenses internacionais, o cumprimento das etapas essenciais no processo de coleta e preservação da prova digital, são primordiais, pois a etapa de isolamento efetivo, permite a geração de uma informação confiável, para possibilitar um espelhamento técnico detalhado, e por fim, preservar esta informação através de um meio que assegure a identificação do emissor, a sua integridade e anterioridade (MUNHOZ, 2021).

Diante da volatilidade da preservação das provas digitais, em virtude dos dados ou dos metadados relacionados poderem ser facilmente manipulados, seja por motivos decorrentes do próprio usuário, de forma intencional ou não, ou em razão do sistema operacional, o conceito de cadeia de custódia apresentado pela Lei n. 13.964/2019 é "*em suma, a sistematização de procedimentos que objetivam a preservação do valor probatório da prova pericial caracterizada, mais precisamente, da sua autenticidade*" (CUNHA, 2020, p. 174). Segundo Rogério Cunha (2020), a prova pericial que de forma precisa observa a cadeia de custódia pode ser considerada uma prova probante, assumindo caráter singular frente ao juízo.

Diante do acima exposto, sendo a prova digital uma prova não documental, que deve ser aferida através de métodos técnicos científicos, faz-se necessário a padronização do seu tratamento de coleta e preservação, em conformidade com as leis, normas e regulamentos forenses internacionais, e consequentemente com o efetivo cumprimento das 03 (três) fases essenciais para a coleta e preservação da prova digital dentro do processo da cadeia de custódia digital, com vistas a garantir a integridade e autenticidade desta prova e sua credibilidade em juízo.

4.2 FERRAMENTA *VERIFACT* X *BLOCKCHAIN* COMO PROVA DIGITAL CONFIÁVEL

Para melhor abordagem do tema, será exposto o comportamento e o funcionamento de uma das ferramentas de registro de evidências digitais, disponível no mercado atualmente, que pode ser usada em processos judiciais, denúncias, acordos e outros fins, bem como trataremos da sua validade jurídica e realizaremos uma breve comparação com a *Blockchain* como prova digital confiável.

Antes de adentrarmos nesta análise e reforçando o que foi abordado no capítulo 2 deste trabalho, ressaltamos que de acordo com Ada Pellegrini Grinover, "*não haveria limitações ou restrições à admissibilidade de quaisquer meios para a produção de provas"* (2012, pg. 386). A autora ressalta que nesse sentido, o Código de Processo Penal, em seu art. 155, *"contém implícita a adoção do princípio da liberdade dos meios de prova*" (BRASIL, 1941). O Código de Processo Civil, outrossim, dispõe que todos os meios legais, bem como todos os outros não especificados em lei, desde que moralmente legítimos, *"são hábeis para provar a verdade dos fatos em que se funda a ação ou a defesa"* (BRASIL, 2015).

A ferramenta em análise, chama-se VERIFACT, conforme parecer jurídico dos advogados Vicente Takaji Suzuki (OAB/PR 38.848) e Hugo Fernando Men Lopes (OAB/PR 86.989), trata-se de uma plataforma fundamentada *"em base científica sólida, capaz de viabilizar uma verificação esclarecedora do fato ocorrido em ambiente digital, e, ao mesmo tempo, constituir sobre a prova uma blindagem contra fraudes e manipulações"* (SUZUKI E LOPES, 2019, p.9).

Com vistas a análise da VERIFACT, à luz do cumprimento das etapas essenciais para coleta e preservação das provas, examinaremos se a ferramenta respeita os princípios da cadeia de custódia previstos na Lei 13.964/2019, bem como a Norma ABNT NBR ISO/IEC 27037:2013, que é padrão internacional, e fornece diretrizes específicas no manuseio de evidências digitais.

Em seu site a VERIFACT (2022) afirma que:

> "[...] possui validações realizadas por empresas especializadas independentes sobre seu sistema e efetividade no cumprimento ao que se propõe: realizar capturas técnicas de provas digitais para processos judiciais. A palavra validação, segundo definição da norma técnica internacional, ISO 9000, significa confirmar, através de fornecimento de evidência objetiva, que

> requisitos para o uso específico pretendido, ou para uma aplicação, foram atendidos" (VERIFACT, 2022).

Analisando o parecer técnico da SIPERCOM (2019, p.14), empresa do ramo de segurança da informação e de consultoria em tecnologia, que realizou uma análise focada na metodologia e entregas da plataforma da VERIFACT, descreveu em seu relatório que:

> "(…) Ao comparar com um documentos de fé pública, considerando seu conteúdo meramente narrativo com produção de prova de existência, o resultado produzido pela Plataforma Verifact, no caso específico que ela se propõe a registrar, **pode ser considerado mais consistente e confiável que o registro feito em tabeliães na atualidade, visto as boas práticas forenses que permitem uma avaliação acurada por um perito especializado ou assistente técnico, medidas de segurança para prevenir fraudes, metodologia utilizada de registro e preservação, e por fim, uma prova de existência também feita por meio regulamentado no país** (**carimbo de tempo ICP/Brasil**)"(SIPERCOM, 2019, p.14, grifo nosso).

Diante da afirmação técnica acima de que a VEFIFACT permite medidas de segurança para **prevenir fraudes** (Primeira Fase - Isolamento, princípio do Isolamento), **metodologia utilizada de registro** (Segunda Fase - Coleta técnica detalhada, princípio do reconhecimento, fixação e coleta), **preservação e prova de existência através do carimbo de tempo ICP/Brasil** (Terceira Fase - Preservação, princípio do acondicionamento), afere-se que conforme parecer técnico, a VERIFACT cumpre os princípios do **Isolamento, reconhecimento, fixação, coleta e acondicionamento,** previsto na Lei 13.964/2019 (pacote anticrime), relativos à coleta e preservação da cadeia de custódia digital, bem como com as diretrizes constantes na Norma ABNT NBR ISO/IEC 27037:2013, e consequentemente com as 03 (três) fases essenciais para a coleta e preservação da prova digital: **Isolamento, Coleta técnica detalhada e Preservação**.

A ferramenta VEFIFACT (2022) afirma que:

> Procura atender as recomendações aplicáveis da ABNT NBR ISO/IEC 27037, documento validado internacionalmente com orientações para se obter confiança nas evidências digitais.
> A plataforma também permite o cumprimento dos 5 passos relativos à coleta e preservação da Cadeia de Custódia previstas na Lei 13.964/2019 (pacote anticrime)
> • **Reconhecimento**: em conjunto com o usuário, que direciona os conteúdos à serem registrados, enquanto a ferramenta busca dados técnicos sobre a situação;

> • **Isolamento**: coleta em ambiente controlado e isolado de interferências de outras atividades, com medidas efetivas para evitar a intervenção e uso de ponto de acesso seguro à internet;
> • **Fixação**: descrição dos dados com origem, data de registro em horário local e UTC, códigos hash individuais para cada arquivo e outros;
> • **Coleta**: registro de imagens, vídeos, áudios e arquivos, com a coleta de metadados técnicos. O resultado é gravado em formatos abertos e facilmente acessíveis;
> • **Acondicionamento**: armazenamento dos dados com selo que garante a integridade posterior do material, realizado com o recurso da Certificação Digital ICP/Brasil (Assinatura Verifact + Carimbo de Tempo). (VEFIFACT, 2022).

Examinando o Parecer técnico, emitido pelo especialista em segurança da informação e privacidade da EarlySec, Wagner Monteverde (2019), que realizou uma auditoria da VERIFACT, referente a aplicação técnica de métodos de captura de informações, interface de usuário, arquitetura de servidores, métodos e protocolos de comunicação internos da infraestrutura, tecnologias utilizadas, dependências de terceiros e mecanismos antifraude, colaciona que a plataforma:

> "Possui uma infraestrutura robusta, com mecanismos antifraude consistentes, mecanismos de criptografia quântica, tratamento de erros, camada de proteção contra atacantes e verificação **capazes de garantir a confidencialidade, integridade e disponibilidade da aplicação e das informações contidas na mesma**. A aplicação quando comparada a outras arquiteturas têm alto grau de complexidade e mecanismos de segurança. " (MONTEVERDE, 2019). (EarlySec, 2019, grifo nosso).

Nesse sentido, citamos o relatório técnico emitido pela eSecurity cybersecurity (2020, p.4), empresa referência na área de cibersegurança no Brasil, tendo em sua carteira de clientes instituições militares, multinacionais e grandes empresas:

> Foram realizados diversos testes de segurança e tentativas de manipulação no processo de registro de evidências providas pela plataforma. Nesta análise foram encontradas diversas proteções de segurança para evitar ataques simples e sofisticados no processo de coleta de informações fornecido pela plataforma, bem como em outros pontos do sistema.
> A partir do estudo realizado foi constatado que a **Verifact possui medidas efetivas para evitar a manipulação do conteúdo registrado durante e depois de seu processo de registro de evidências digitais**, coletando as informações conforme constam em sua origem. Também foi constatada a efetividade da segurança sobre os dados armazenados e outros pontos detalhados na metodologia descrita em seguida (eSecurity cybersecurity, 2020, p.4, grifo nosso).

Isto posto, os pareceres técnicos se alinham e corroboram ao demonstrar que a plataforma VERIFACT cumpre os princípios da cadeia de custódia digital e atende tecnicamente as diretrizes de confiança da coleta e preservação dos registros de evidências digitais.

Ao realizarmos de forma breve, uma análise da tecnologia *Blockchain*, aplicadas em provas digitais, utilizando como parâmetro o cumprimento das fases essenciais para a coleta e preservação de uma prova de forma confiável e consequentemente os princípios da cadeia de custódia definidos na Lei 13.964/2019, observamos que a *Blockchain*, nas palavras de Alexandre Munhoz (2021), cumpre apenas a **fase da preservação** da prova, que versa sobre o **princípio do acondicionamento** da cadeia de custódia. No entanto, as etapas do **Isolamento** (princípio do isolamento) e da **Coleta técnica detalhada** (princípio do reconhecimento, fixação e coleta) não são cumpridas.

> Afinal, considerando que neste cenário **a capacidade técnica da *Blockchain* cumpre somente os requisitos da preservação**, como exatamente ela contribui para o isolamento contra manipulação do fato original e seu espelhamento técnico detalhado?
> De que autenticidade estamos falando ao considerar uma informação preservada na *Blockchain*, sem procedimentos adequados para gerar um conteúdo confiável antes de seu registro?
> Preservar a integridade e anterioridade de um conteúdo, em que não há argumentos para afirmar sua semelhança com o fato original, gera valor probatório?
> **Para que uma prova preservada na *Blockchain* ou Certificação Digital tenha um conteúdo confiável, é preciso que a informação também tenha confiança antes da sua preservação, portanto, seu valor está condicionado a processos anteriores que gerem uma informação autentica.**
> [...]
> A *Blockchain* é uma ferramenta tecnológica fantástica, que possui funções específicas e cenários onde ela é aplicada com muito sucesso. É fato que ela pode ter um papel importante na preservação das provas digitais como alternativa à Certificação Digital ou Fé Pública, entretanto, **é preciso entender que o valor das provas no ambiente digital depende de outros fatores que vão além da capacidade técnica destes recursos, ou seja, não resolvem a questão sozinhas** (MUNHOZ, 2021, grifo nosso).

Por conseguinte, considerando que a *Blockchain* cumpre apenas umas das fases essenciais da coleta e preservação de uma prova digital, podemos dizer que no direito, a sua utilização ensejaria uma presunção relativa, pois o não cumprimento das etapas de isolamento e de Coleta técnica detalhada, enseja contaminação das provas digitais e possibilita fraudes, comprometendo a cadeia de custódia digital, pois “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 JUNIOR, 2019, p. 493), diante disso, o uso da *Blockchain* aplicada em provas digitais, pode gerar insegurança em relação a sua autenticidade e integridade, pois não seria tecnicamente possível afirmar sua fonte original ou a sua não adulteração em conformidade com o fato inicial.

4.3 CREDIBILIDADE PARA ACEITAÇÃO EM JUÍZO DO RELATÓRIO TÉCNICO EMITIDO POR FERRAMENTA DE COLETA DE METADADOS DE FATOS DIGITAIS

Como tratado no subcapítulo 3.3 deste trabalho, o problema da aceitação da prova digital em juízo é que esta evidência digital pode ser facilmente manipulada, diante da possibilidade de supressões, alterações e exclusões de metadados, diante da sua volatilidade (NETO; SANTOS, 2020), neste sentido o STJ decidiu que o uso de *prints* de conversa de *Whatsapp* estão vedadas como provas digitais.

Desta forma, diante da fragilidade da prova digital, reforça-se a necessidade do efetivo cumprimento das 03 (três) fases essenciais para a coleta e preservação da prova digital dentro do processo da cadeia de custódia digital, para garantia da sua autenticidade, integridade e aceitação em juízo.

Dando continuidade à análise da ferramenta VERIFACT, Vicente Takaji Suzuki e Hugo Fernando Men Lopes (2019, p.7) afirmam que:

> **A plataforma Verifact apresenta-se como solução a essas fragilidades**, posto que viabiliza a captura técnica de fatos ocorridos ou retratados em websites ou aplicações, v. g., redes sociais, plataformas e- commerce, webmail, etc..
> **Essa plataforma foi concebida para oferecer um alto nível de segurança, com medidas que buscam evitar fraudes no conteúdo capturado, justamente para que o resultado final seja um registro claro e passível de validação por meio de eventual perícia técnica** do objeto da captura no ambiente digital - ao contrário do que ocorre, por exemplo, com a ata notarial e os prints de tela (SUZUKI E LOPES, 2019, p.7, grifo nosso).

Congruente exposto no capítulo anterior, a ferramenta VERIFACT cumpre os princípios da cadeia de custódia digital e atende tecnicamente as diretrizes de confiança da coleta e preservação dos registros de evidências digitais, pois é aderente à ISO 27037, que é a diretriz para identificação, coleta, aquisição e preservação de

evidência digital, neste diapasão, iremos abordar o conteúdo do relatório técnico emitido pela ferramenta e juntado aos autos como prova digital em juízo.

Conforme consulta ao site da VERIFACT (2022), eles afirmam que a ferramenta permite a coleta de provas digitais que podem ser auditadas e com validade jurídica, e que a referida coleta pode ser feita pelo próprio usuário de forma intuitiva e ágil. Segundo o referido site, é possível realizar a coleta de imagens, áudios, vídeos, textos e diversos arquivos em outros formatos. Declaram também, que a ferramenta é acessível por navegador de internet, bem como por aplicativos como *Whatsapp* e telegram, redes sociais (Tik tok, Instagram, *Facebook*, *Twitch, Twitter* e outros), plataforma de vídeos (youtube e vimeo), webmails e sites.

A coleta dos dados digitais resulta na emissão de um relatório técnico, auditável, com garantia da imutabilidade dos dados, com possibilidade futura de ampla perícia técnica das informações coletadas (VERIFACT, 2022, s/p):

> O resultado é a **emissão de um relatório técnico** certificado com as telas registradas, dados e **metadados técnicos auditáveis** para uma eventual perícia técnica, além de um vídeo de registro da navegação, com áudio, além de arquivos baixados durante a sessão.
> O relatório técnico leva a assinatura certificada da Verifact e carimbo de tempo ICP-Brasil. **O carimbo de tempo ICP-Brasil**, ou timestamp utilizado no relatório **gera imutabilidade dos dados**, registrando o exato dia e horário que o conteúdo foi acessado na internet e impedindo que os dados sejam apagados ou alterados após o registro.
> Até mesmo se o conteúdo original desaparecer da Internet, com os dados e metadados coletados **é possível realizar ampla perícia técnica das informações**, para comprovar que o material é aquilo que diz ser e vem de onde diz ter vindo.
> É importante que o conteúdo seja coletado a partir da fonte original. Arquivos e mensagens reencaminhadas ou salvas em outros locais não são recomendáveis, pois perdem dados e informações importantes para comprovar a origem e integridade (VERIFACT, 2022, grifo nosso).

De acordo com parecer técnico da SIPERCOM (2019, p.2), empresa de consultoria em tecnologia e segurança da informação, que realizou uma análise focada na metodologia e entregas da plataforma da VERIFACT, concluiu-se que, o relatório técnico, emitido pela referida ferramenta é considerado válido e consistente o suficiente para os fins aos quais se destina. O parecer ressaltou que “[...] *de posse de cópias do relatório técnico e dos demais artefatos produzidos na captura, o indivíduo poderá fazer uso deles, mesmo que a plataforma não esteja disponível, por qualquer motivo ou que a captura já tenha sido removida da plataforma; ”.*

A SIPERCOM afirma que a ferramenta aplica "*técnicas de aquisição e preservação de evidências digitais semelhantes àquelas utilizadas em investigações e perícias e, agregando garantias de integridade aos dados coletados e ao relatório técnico produzido*". Para garantia de integridade do relatório técnico, a plataforma utiliza certificação digital e carimbo de tempo vinculados à ICP-Brasil (Medida Provisória nº 2.200-2). A empresa concluiu que o método de validação manual da integridade do relatório técnico funciona adequadamente, e que a técnica de controle de integridade dos dados é bastante efetiva e largamente utilizada no âmbito de perícias digitais.

Diversas empresas e Órgãos da Justiça vem utilizando a plataforma da VERIFACT para coleta de prova digital, como exemplo citamos o Ministério Público do Estado da Bahia (MP-BA), que firmou Termo de cooperação mútua, Processo SEI:19.09.02251.0005160/2020-94. Averiguando o atestado de capacidade técnica emitido pelo MP-BA (2021, pg.1), o Órgão atesta que a ferramenta atende os requisitos efetivos referentes as 03 fases essências para a coleta e preservação da prova digital dentro do processo da cadeia de custódia digital.

Especificamente em relação ao relatório técnico emitido pela plataforma, concernente a fase da preservação, a terceira fase, eles atestam que o documento é gerado no formato PDF/a, respeitando as normas internacionais e que o mesmo é preparado para o arquivamento de longo prazo:

> Quanto à preservação:
> • Preservação de integridade e anterioridade do relatório gerado com o uso de Certificação Digital ICP/Brasil, gerido pelo governo brasileiro/Instituto Nacional de Tecnologia da Informação (MP 2.200-2), que gera forma de verificação regulamentada, independente da empresa prestadora de serviços e com governança de longo prazo;
> • Uso de Certificado ICP/Brasil A3 da Verifact para a identificação da origem do relatório, bem como o uso do recurso Carimbo de Tempo ICP/Brasil, para geração de referência temporal na geração do relatório;
> • Preservação da integridade dos arquivos externos ao relatório com o uso de cálculos HASH SHA512 e SHA3-512, que por sua vez, são protegidos pela certificação no relatório PDF;
> • Identificação de origem e momento do registro dos conteúdos em fuso horário local e em formato UTC;
> • **Geração de relatório em formato PDF/A, baseado na norma ISO 19005-2, que busca garantir a integridade do documento diante da evolução tecnológica do formato PDF ao passar dos anos** (MP-BA, 2021, grifo nosso).

O MP-BA atesta ainda, que a plataforma VERIFACT, em relação à interface de uso, é amigável para usuários que não possui conhecimento técnico avançado, gera um resultado rápido e automatizado, e afirma que a plataforma prestou o serviço e entregou os materiais com excelente desempenho operacional, cumprindo fielmente as obrigações, e que não foi registrado nenhuma desconformidade técnica ou comercial, além do mais, a parceria gerou benesses para instituição como (2021, pg.2):

> • **Agilidade no atendimento das etapas da Cadeia de Custódia referente à coleta e preservação de evidências digitais, além das boas práticas previstas na ABNT NBR ISO/IEC 27037:2013, para itens aplicáveis na situação em questão**;
> • Redução do tempo gasto do agente na operação de coleta e preservação de provas digitais em websites;
> • Atendimento de requisitos de segurança internos ao dispensar a instalação de software em computadores da instituição;
> • Redução significativa de custos com a coleta e preservação de evidências digitais;
> • Confiabilidade e confidencialidade em relação a guarda de informações/dados sensíveis (MP-BA, 2021, grifo nosso).

Por tanto, mais uma vez estamos diante da afirmação de que a ferramenta VERIFACT atende as fases da cadeia de custódia referente à coleta e preservação de evidências digitais, bem como as diretrizes previstas na ABNT NBR ISO/IEC 27037:2013, neste sentindo o delegado Higor Jorge (2020, p. 134 e 135), da Polícia Civil de São Paulo, afirma que "*A VERIFACT é uma plataforma on-line que permite a captura e a preservação de técnica de fatos ocorridos no ambiente online (...), automatizando práticas comuns na área forense digital e medidas técnicas efetivas contra fraude e manipulação no processo de registro*".

Tendo em vista que a ferramenta VERIFACT é válida e adequada à legislação vigente e possui bases técnicas sólidas para manifestar, em juízo, a realidade de fatos ocorridos na internet, conforme demonstrado no presente capítulo, iremos verificar processos que estão em andamento no judiciário brasileiro que fizeram uso da ferramenta, bem como decisões judiciais que aceitaram a prova digital decorrente da mesma, demonstrando que o relatório técnico emitido pela plataforma tem sido aceito em ações judiciais.

Conforme site da VERIFACT (2022) a ferramenta foi utilizada nas seguintes ações judiciais:

- **Instância superior**
    - **AgRg no Habeas Corpus nº 683483 - PR (2021/0240089-1)** (PENAL/Decisão de 1º grau mantida, onde a materialidade foi comprovada a partir do relatório da VERIFACT)

- **2º grau**
    - Processo RE 060024946 – TRE-PI

- **1º grau**
    - ATOrd 1000573-49.2020.5.02.0063 TRT SP – 63ª VARA DO TRABALHO
    - ATOrd 0000009-55.2021.5.12.0037 TRT SC
    - Processo 1007756-16.2019.8.26.0604 – TJSP
    - Processo 0077695-06.2019.8.16.0014 – TJPR
    - Processo 0005581-34.2019.8.16.0058 – TJPR
    - Processo 1051245-29.2020.8.26.0100 – TJSP
    - + Diversos outros que correm em segredo de justiça

Recentemente o Superior Tribunal de Justiça (STJ), proferiu acórdão nos autos do AgRg no Habeas Corpus nº 683483 - PR (2021/0240089-1), expondo que a ferramenta VERIFACT foi decisiva como prova digital, pois no caso em tela, o impetrante do habeas corpus pleiteava o relaxamento da sua prisão preventiva, alegando que não existia provas que demonstrassem o indício da autoria dos crimes, porém o entendimento do Tribunal de Justiça do Paraná e do STJ foi que as provas eletrônicas apresentadas com o auxílio da VERIFACT eram suficientes para indicar a autoria do crime e a ocorrência dele.

O relator, Ministro João Otavio de Noronha, destacou trecho da decisão do Tribunal de Justiça do Paraná, que salientou que as provas obtidas com certificação da VERIFACT eram satisfatórias e legítimas:

> “Na hipótese, está justificada a decretação da custódia provisória do agravante, pois foi demonstrada pelo Juízo de primeiro grau, de forma motivada, a presença dos requisitos previstos nos arts. 312, 313 e 315 do CPP. A propósito, confira-se excerto do decisum que decretou a prisão cautelar (fls. 88- 89):

> Da detida análise dos autos, verifica-se que a materialidade delitiva e os indícios de autoria restaram suficientemente demonstrados por meio do boletim de ocorrência e documentos juntados em sede policial (mov. 1.3/1.13).
>
> Veja-se os fatos relatados pela noticiante no Boletim de Ocorrência: "A NOTICIANTE *CLEUSA ROSANE RIBAS FERREIRA* TEVE UM ENVOLVIMENTO EMOCIONAL COM O NOTICIADO *TARCISIO SILVEIRA DA MAIA*. ESTA RELAÇÃO PERDUROU POR 01 ANO, E SE ENCERROU HÁ 01 ANO. NÃO RESIDE JUNTO COM O AGRESSOR. INFORMA *CLEUSA ROSANE RIBAS FERREIRA* QUE, EM 09/06/2021, ÀS 12:45, NA RUA ALAMEDA CABRAL, 665, CENTRO, CURITIBA # PR, CASA DA VÍTIMA, *TARCISIO SILVEIRA DA MAIA* A EXTORQUE FINANCEIRAMENTE DIZENDO: #VOCÊ É UMA VAGABUNDA, ESTRAGOU MINHA VIDA, VOCÊ TEM QUE PAGAR POR TER ESTRAGADO MINHA VIDA, QUERO 70 MIL AGORA DE TARDE, QUERO QUE VOCÊ DEPOSITE DE TARDE#. PERSEGUE LIGANDO EM MÉDIA 150 VEZES POR DIA VIA APLICATIVO *WHATSAPP*. OFENDE: #VAGABUNDA, DESGRAÇADA, LACRAIA# A NOTICIANTE SE SENTIU OFENDIDA DIANTE DE TAL DECLARAÇÃO. AMEAÇOU DIZENDO A SEGUINTE FRASE: #O BAGULHO VAI FICAR LOCO, SÓ NÃO SENTEI O PREGO AINDA EM VOCÊS DOIS, ME ATENDA QUE É MELHOR, VOCÊ NÃO SABE COM QUEM MEXEU, VOU SER MUITO PIOR# A NOTICIANTE SENTIU-SE AMEAÇADA DIANTE DAS DECLARAÇÕES. TEME POR SUA INTEGRIDADE FÍSICA. **(CERTIFICAÇÃO DIGITAL VERIFACT).** ISSO OCORREU PORQUE, SEGUNDO A VÍTIMA, O NOTICIADO SE PREVALECE PELA VÍTIMA SER UMA PESSOA PÚBLICA. A NOTICIANTE REQUER AS MEDIDAS PROTETIVAS DE URGÊNCIA APÓS TER SIDO INFORMADA DOS DIREITOS A ELA CONCEDIDOS PELA LEI 11.340/06.
>
> [...] **As alegações da vítima foram precedidas das provas por meio da mídia "verifact" de mov. 1.7/1.8. Evidenciam-se, portanto, indícios de autoria e materialidade delitivas suficientes para o exame da prisão cautelar. Presente, assim, o fumus comissi delicti.**
> (…)
> Diante da gravidade dos fatos ocorridos, verifica-se que não há outra medida jurídica cabível a não ser a manutenção da prisão preventiva, sendo o encarceramento provisório medida necessária e proporcional à conduta praticada, como forma de garantia da ordem pública".
> O Juízo de primeiro grau demonstrou, de forma motivada, a presença dos requisitos autorizadores da segregação cautelar, previstos nos arts. 312, 313 e 315 do CPP, notadamente a gravidade concreta dos delitos, o modus operandi empregado para a execução e a periculosidade do paciente, de modo que não há falar em constrangimento ilegal" (STJ - HC: 683483 PR 2021/0240089-1, Relator: Ministro JOÃO OTÁVIO DE NORONHA, Data de Publicação: DJ 08/10/2021). (BRASIL, 2021, grifo nosso).

Por conseguinte, verifica-se que a coleta da prova digital por meio da ferramenta VERIFACT foi fundamental para decisão proferida pelo Tribunal de Justiça do Paraná, bem como pelo STJ em sede de recurso, demonstrando que o relatório técnico emitido tem sido aceito em ações judiciais em todas as instâncias, inclusive por Tribunal Superior, o que evidencia que a prova digital, como prova não documental, obtida na realidade, tem sua autenticidade fundamentada por métodos técnico científicos de coleta e preservação.

Analisando decisão da 2ª Turma do Supremo Tribunal Federal (STF) nos autos da Reclamação nº 32.722 Mato Grosso, no ano de 2019, cuja a numeração única é: 0083429-43.2018.1.00.0000, de Relatoria do Ministro Gilmar Mendes, observamos que por maioria de votos, julgou-se procedente a reclamação nos termos do voto do Relator, com base na dúvida sobre a confiabilidade dos dados interceptados juntados aos autos, bem como a necessidade de preservação da cadeia de custódia:

> Conforme informações prestadas pelo Juízo de origem, "os elementos colhidos nos autos indicam que as alegadas edições/inserções realizadas pela Polícia Federal se restringiam ao cabeçalho dos diálogos, para fins de facilitação da investigação, e não em relação aos respectivos conteúdos". Ademais, "o cabeçalho é totalmente independente do conteúdo das mensagens. Conforme informou a testemunha William de Oliveira Dias, em sua oitiva judicial, no momento em que as mensagens eram descriptografadas, o programa permite no cabeçalho a identificação do investigado que seria o interlocutor do diálogo pertencente àquele ID". (eDOC 202, p. 11)
>
> Desse modo, por um lado, estabeleceu-se uma **situação de dúvida, embasada em elementos concretos, sobre a confiabilidade dos dados** apresentados pela autoridade investigatória em relação às comunicações interceptadas. Assim, a incerteza sobre a fidedignidade das investigações impõe a adoção de medidas para proteção da **cadeia de custódia** das informações.
>
> Na doutrina, afirma-se que "um dos aspectos mais delicados da aquisição de fontes de prova consiste em preservar a idoneidade de todo o trabalho que tende a ser realizado sigilosamente, em um ambiente de reserva que, se não for respeitado, compromete o conjunto de informações que eventualmente venham a ser obtidas dessa forma" (PRADO, Geraldo. Prova penal e sistema de controles epistêmicos. São Paulo: Marcial Pons, 2014. p. 77). (BRASIL, 2019, grifo autorais).

No processo em análise, segundo o relator, diante da insegurança quanto à autenticidade da prova apresentada pela acusação, tem-se motivo suficiente para assegurar que a defesa tenha acesso aos arquivos que foram originalmente usados para a incriminação de uma pessoa. O advogado do reclamante, que de acordo com os autos era investigado por crime contra o sistema financeiro nacional e por lavagem de dinheiro, alegou que as mensagens enviadas via Blackberry (linha de smartphones criada pela empresa canadense BlackBerry, com foco no mercado corporativo) e usadas pela acusação como prova, foram alteradas pela Polícia Federal.

> Nesse sentido, **"a preservação de cada uma das etapas da operação que realizou a interceptação das comunicações de um cidadão (cadeia de custódia) é a única maneira de assegurar a integridade do procedimento**

> **probatório, permitindo que a defesa rastreie e conheça as fontes de prova".** (SANTORO; TAVARES; GOMES. O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. Revista Brasileira de Direito Processual Penal, v. 3,. n. 2, 2017.p. 628)
>
> Segundo a autoridade reclamada, "a inserção do nome dos acusados ao lado do Nickname ou do ID, não caracteriza alteração do conteúdo das mensagens, pelo contrário, foi uma forma de efetivar o direito à informação dos réus, corolário dos princípios do contraditório e da ampla defesa, viabilizando as defesas dos acusados". (eDOC 202, p. 15)
> Sem dúvidas, a reconhecida alteração dos cabeçalhos não comprova, automaticamente, modificações no conteúdo das interceptações. **Contudo, destaco que os arquivos eram editáveis pelas autoridades investigativas. E essa é a questão problemática aqui analisada.** (BRASIL, 2019, grifo nosso).

O Juízo de origem afirma que as edições feitas pela Policia Federal ocorreram com vistas a facilitar a investigação e foram realizadas somente nos cabeçalhos, o que não permitiu atingir o conteúdo das mensagens, e dessa forma não teria sido possível a alteração no fluxo de dados do arquivo.

> O exercício do poder punitivo estatal pressupõe a existência de uma condenação proferida após o transcurso de um processo penal com o devido respeito aos direitos e às garantias fundamentais. Trata-se de premissa essencial à aplicação de uma pena: **os atos estatais precisam ser confiáveis.**
>
> **Se há a caracterização de um cenário de dúvida sobre a confiabilidade e a fidedignidade de atos dos atores envolvidos com a persecução penal, deve-se adotar medidas para resguardar a legitimidade de tal atuação**. Nesse caso, como relatado pela própria autoridade policial, há a possibilidade de acesso aos arquivos originais, sem maiores dificuldades ou prejuízo para o andamento do processo.
>
> Diante do exposto, julgo procedente esta reclamação, reconhecendo a violação aos termos da Súmula Vinculante 14, deste Tribunal, para assegurar à defesa o acesso aos arquivos originais das interceptações telemáticas, consoante fornecido pela operadora BlackBerry. (STF - Rcl 0083429-43.2018.1.00.0000 MT - MATO GROSSO 0083429-43.2018.1.00.0000, Relator: Ministro GILMAR MENDES, Data de Publicação: DJ 29/11/2019). (BRASIL, 2019, grifo nosso)

Como afirmado pelo Ministro relator, os atos do estado precisam ser confiáveis, e havendo dúvida, adota-se medidas para resguardar a legitimidade, nesse sentido, sendo a prova digital uma prova não documental e que deve ser aferida por meios técnicos, essa afirmação do juízo de origem de que as edições feitas pela Policia Federal não atingiram o conteúdo das mensagens, só seria possível se a prova utilizada tivesse cumprindo o princípio aplicável aos documentos digitais,

considerando suas especificidades e complexidades, para garantir que não houve ruptura de sua custódia, desde o isolamento, coleta e preservação.

Logo, necessariamente a prova digital precisa cumprir as etapas essenciais da cadeia de custódia para assegurar sua autenticidade, confiabilidade, integridade e fixidez ao longo do tempo, em uma abordagem de Preservação Digital Sistêmica (FLORES, 2020, slide 36). Considerando que a ferramenta VERIFACT cumpre a cadeia de custódia da prova digital, podemos hipoteticamente pensar que se a Polícia Federal houvesse utilizado a citada ferramenta, seria possível inferir que a cadeia de custódia da prova em análise não seria quebrada.

Por consequência, tendo em mente que “A cadeia de custódia é um processo usado para manter e documentar a história cronológica da evidência, para garantir a idoneidade e o rastreamento das evidências utilizadas em processos judiciais” (LOPES et al, 2006, p. 1), para que a prova digital seja considerada autêntica e íntegra, deve ser cumprida as 03 (três) fases essenciais para sua coleta e preservação dentro do processo da cadeia de custódia previstos na Lei 13.964/2019, bem como deve ser respeitada a Norma ABNT NBR ISO/IEC 27037:2013, que é padrão internacional, e fornece diretrizes específicas no manuseio de evidências digitais, visando que essa prova digital tenha credibilidade em juízo.

Neste diapasão, diante de todo o exposto, constata-se que o relatório técnico emitido pela ferramenta VERIFACT é adequado e está em conformidade com a legislação vigente e com as normas e regulamentos forenses internacionais, bem como é aceito em diversos casos e instâncias judiciais, é atualmente adequado para coletar e preservar as provas digitais obtidas na realidade de fatos ocorridos na internet, de forma a garantir-lhe força probante e credibilidade em juízo.

5 CONSIDERAÇÕES FINAIS

O desenvolvimento do presente estudo possibilitou uma análise de como a execução da coleta de registros digitais pode garantir a autenticidade probatória à prova digital, uma reflexão acerca dos benefícios da aplicação dos princípios da cadeia de custódia, previstos na Lei 13.964/2019, com vistas a manutenção do histórico de forma cronológica das evidências digitais, com o propósito de garantir a idoneidade e o rastreamento dessas evidências utilizadas em processos judiciais.

De um modo geral, a pesquisa demonstrou que o novel da prova digital é de grande relevância nos processos judiciais, seja na esfera penal, civil, administrativa e outras, e sendo esta uma prova obtida a partir de documentos não formais, adquirida na realidade dos fatos, necessita-se de métodos técnicos que proporcionem garantir um material probatório confiável, utilizando registros digitais para auxiliar magistrados, advogados e partes na instrução processual.

Cada vez mais os tribunais vem concretizando em suas decisões que não basta que a prova digital seja lícita, mas que deve ser assegurada a sua autenticidade, que no caso em análise deve ser demonstrada por meio do cumprimento dos passos essenciais a serem executados na coleta de metadados detalhados de fatos digitais, mediante a cadeia de custódia digital, bem como respeitando a Norma ABNT NBR ISO/IEC 27037:2013, que é padrão internacional, e fornece diretrizes específicas no manuseio de evidências digitais, visando que essa prova digital tenha credibilidade em juízo.

No entanto, o problema da aceitação da prova digital em juízo é que esta evidência digital pode ser facilmente manipulada, pois é tecnicamente possível falsifica-la de diversas formas, desde SMS, bate-papos no Whastapp, e-mails ou postagens em redes sociais, e diante da falta de regulamentação em relação a cadeia de custódia das provas digitais de forma a abranger qualquer fonte de prova de natureza real, gera-se uma dificuldade na resolução de crimes em ambientes digitais, bem como constitui-se uma insegurança jurídica, já que a falta de uma padronização legal em relação a coleta de evidências digitais, permite que provas legais, mas não autênticas sejam acolhidas em processos, possibilitando que decisões judiciais sejam fundamentadas em provas que se distanciam da verdade real dos fatos.

Mesmo diante da falta de uma regulamentação em relação a cadeia de custódia das provas digitais, considerando que a lei 13.964/2019, conhecida como o pacote anticrime, consolidou os 05 princípios da cadeia de custódia que versam sobre as fases essenciais para a coleta e preservação de uma prova de forma confiável e temos ainda a Norma ABNT NBR ISO/IEC 27037:2013, que tem como objetivo padronizar o tratamento das evidências digitais, verificamos que em conformidade com a lei e regulamentações floresce internacionais, consolida-se que para uma prova digital ser considerada autêntica, faz-se mister o cumprimento efetivo das 03 (três) fases essenciais para a coleta e preservação da prova digital dentro do processo da cadeia de custódia digital, as quais são: A primeira fase é o Isolamento; A segunda fase é a Coleta técnica detalhada e a terceira fase é a Preservação.

A análise da VERIFACT, ferramenta de registro de evidências digitais disponível no mercado atualmente, utilizada em processos judiciais, administrativos, denúncias, acordos e outros fins, demonstrou conforme pareceres técnicos da SIPERCOM, empresa de consultoria em tecnologia e segurança da informação; da Earlysec, empresa de segurança e inteligência cibernética; da eSecurity cybersecurity empresa referência na área de cibersegurança no Brasil; atestado de capacidade técnica emitido pelo Ministério Público da Bahia (MP-BA); bem como conforme pareceres jurídicos dos advogados Vicente Takaji Suzuki (OAB/PR 38.848) e Hugo Fernando Men Lopes (OAB/PR 86.989), que cumpre os princípios da Cadeia de Custódia digital e atende tecnicamente as diretrizes de confiança da coleta e preservação dos registros de evidências digitais.

Em uma breve análise comparativa da VERIFACT com a *Blockchain* como prova digital confiável, verificou-se que a *Blockchain* cumpre apenas umas das fases essenciais da coleta e preservação de uma prova digital, destarte no direito, a sua utilização ensejaria uma presunção relativa, pois o não cumprimento das etapas de isolamento e de coleta técnica detalhada, gera contaminação das provas digitais e possibilita fraudes, comprometendo a cadeia de custódia digital, provocando insegurança em relação a sua autenticidade e integridade.

A ferramenta VERIFACT é válida e adequada à legislação vigente e possui alicerces técnicos sólidos para, em juízo, apresentar a realidade de eventos (fatos) ocorridos em meios digitais.

Desse modo, o presente trabalho analisou processos que estão em andamento no judiciário brasileiro que fizeram uso da ferramenta, bem como decisões

judiciais que aceitaram a prova digital decorrente da mesma, demonstrando que o relatório técnico emitido pela plataforma tem sido aceito em ações judiciais, inclusive sendo fundamental para decisão proferida pelo Tribunal de Justiça do Paraná, bem como pelo Superior Tribunal de Justiça em sede de recurso, nos autos do AgRg no Habeas Corpus nº 683483 - PR (2021/0240089-1).

Dada à relevância do tema, torna se necessário o desenvolvimento de pesquisas que visem analisar decisões judiciais que foram fundamentadas em provas digitais ou deixaram de acolhe-las, averiguando se as provas utilizadas cumpriram os princípios do isolamento, reconhecimento, fixação, coleta e acondicionamento, previsto na Lei 13.964/2019 (pacote anticrime), relativos à coleta e preservação da Cadeia de Custódia digital, bem como com as diretrizes constantes na Norma ABNT NBR ISO/IEC 27037:2013, e consequentemente com as 03 (três) fases essenciais para a coleta e preservação da prova digital. Buscando verificar se foi garantida a confiabilidade da prova digital fornecida em um julgamento.

Nesse sentido, o cumprimento das 03 (três) fases essenciais para a coleta e preservação da prova digital: Isolamento, Coleta técnica detalhada e Preservação, permitem assegurar a autenticidade de documentos eletrônicos, o que possibilita meios de prova digital de credibilidade para solução de controvérsias, uma possível agilidade à tramitação processual e maior proximidade da verdade real dos fatos. Existem ferramentas confiáveis no mercado e acessíveis, a exemplo da ferramenta VERIFACT, capaz de viabilizar uma verificação esclarecedora do fato ocorrido em ambiente digital, e, ao mesmo tempo, proteger a prova de fraudes e manipulações, cumprindo a Cadeia de Custódia digital e atendendo tecnicamente as diretrizes de confiança da coleta e preservação dos registros de evidências digitais.

REFERÊNCIAS

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

ACMINAS. É Ilícita Prova Obtida por meio de Prints do *Whatsapp* Web, Decide Superior Tribunal de Justiça. **ACMinas**, 2022. Disponível em: https://acminas.com.br/e-ilicita-prova-obtida-por-meio-de-prints-do-whatsapp-web-decide-superior-tribunal-de-justica/#:~:text=O%20Superior%20Tribunal%20de%20Justi%C3%A7a%20determinou%20que%20prints,manipuladas%2C%20j%C3%A1%20que%20as%20mensagens%20podem%20ser%20apagadas. Acesso em 20 mar. 2022.

ALMEIDA, Diogo Assumpção Rezende de; FARIA, Marcela Kohlbach. **Processo Civil: Procedimentos. 2015**. FGV. Disponível em: https://direitorio.fgv.br/sites/direitorio.fgv.br/files/u100/processo_civil_-_procedimentos_2015-1.pdf. Acesso em 15 mar 2022.

AZEVEDO, Antonio Danilo Moura de. A teoria dinâmica de distribuição do ônus da prova no direito processual civil brasileiro. **Jus.com.br**, 2007 Disponível em: http://jus.com.br/artigos/10264/a-teoria-dinamica-de-distribuicao-do-onus-da-prova-no-direito-processual-civil-brasileiro/2. Acesso em 15 mar 2022.

BRASIL. **Constituição Federal de 1988**, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 mar. 2022.

BRASIL. Supremo Tribunal Federal. **RECLAMAÇÃO 32.722 MATO GROSSO.** Relator: MIN. GILMAR MENDES DJ:19/11/2019. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5601131. Acesso em: 13 abr. 2022.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA - STJ **- HC: 705770 RJ 2021/0360804-9,** Relator: Ministro RIBEIRO DANTAS, Data de Publicação: DJ 01/02/2022a. Disponível em: https://processo.stj.jus.br/processo/pesquisa/. Acesso em: 22 abr. 2022.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA - STJ **- HC: 718849 SP 2022/0015519-6,** Relator: Ministro JORGE MUSSI, Data de Publicação: DJ 26/01/2022b). Disponível em: https://processo.stj.jus.br/processo/pesquisa/. Acesso em: 22 abr. 2022.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA - STJ - **AgRg no HABEAS CORPUS Nº 683483 - PR 2021/0240089,** Relator: Ministro JOÃO OTÁVIO DE NORONHA**,** Data de Publicação: DJ 08/10/2021). Disponível em: https://www.stj.jus.br/sites/portalp/Processos/Consulta-Processual. Acesso em: 30 mar. 2022.

BRASIL. MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA. **Atestado– 07/10/2021.** Disponível em: https://www.verifact.com.br/wp-content/uploads/2021/10/Atestado_SEI_19.09.01970.0016798_2021_65.pdf. Acesso em 26 mar 2022.

BRASIL. **Lei n.º 13.105, de 16 de março de 2015. Código de Processo Civil**. Portal da Legislação, Brasília, mar. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em 27 ago 2021.

BRASIL. **Decreto Lei n.º 3.689, de 03 de outubro de 1941. Código de Processo Penal**. Portal da Legislação, Brasília. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em 20 fev 2022.

BRASIL**. Lei 13.464, de 24 de dezembro de 2019**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em 15 mar 2022.

CÂMARA DOS DEPUTADOS. **PL 4939/2020**. Disponível em: https://www.camara.leg.br/propostas-legislativas/2264367. Acesso em 20 mar 2022.

CAPOZZI, Ricardo Andrian. A formatação de Provas: coleta e preservação de provas em ambientes digitais e formação da cadeia de custódia ISO 27.037. **Monografias Brasil Escola**, 2019. Disponível em: https://monografias.brasilescola .uol.com.br/direito/formatacao-de-provas-coleta-e-preservacao-de-provas-em-ambientes-digitais-e-formacao-da-cadeia-de-custodia-iso-27037.htm. Acesso em 19 mar 2022.

CAYSE, Eoghan. Digital evidence and computer crime: forensic science, computers, and the Internet. 3ª ed. San Diego/London: **Elsevier Academic Press**, 2011.Tradução livre. ISBN 978-0-12-374268-1. Disponível em: https://books.google. com.br/books?hl=pt-BR&lr=&id=6gCbJ4O4f-IC&oi=fnd&pg=PP2&dq=digital+ evidence+and+computer+crime&ots=Wqp_dB1ug-&sig=3Nx6GFX6lOaA0Ma 1w2aFoH2lYLU#v=onepage&q=digital%20evidence%20and%20computer%20crime &f=false. Acesso em 16 abr. 2022

CUNHA, Rogério Sanches. **Pacote Anticrime: Lei 13.964/2019 – Comentários às alterações no CP, CPP e LEP**. Salvador: JusPodivm, 2020.

DELMANTO JUNIOR, Roberto. Prova documental. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Processo Penal. Marco Antonio Marques da Silva (coord. de tomo). 1. ed. São Paulo: **Pontifícia Universidade Católica de São Paulo**, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/447/edicao-1/prova-documental. Acesso em 19 mar 2022.

DOS SANTOS LUZ, Charlley. Curadoria digital, custódia arquivística e preservação digital: relações possíveis. **Páginas a&b: arquivos e bibliotecas**, p. 92-103, 2018. Disponível em: Disponível em: http://hdl.handle.net/20.500.11959/brapci/109277. Acesso em 18 mar 2022.

EarlySec. Wagner Monteverde. **Parecer técnico**, **29/11/2019.** Disponível em: https://www.verifact.com.br/wp-content/uploads/2020/03/Parecer_auditoria _aplicacao_Verifact-manifesto2019Ax.pdf. Acesso em 19 mar 2022.

EDINGER, Carlos. Cadeia de custódia, rastreabilidade probatória. **Revista Brasileira de Ciências Criminais**, v. 120, p. 237-257, 2016. Disponível em https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2016;100 1128397. Acesso em 18 mar 2022.

eSecurity cybersecurity. Alan Sanches e Evely Macedo. **Relatório Técnico Teste de intrusão em aplicação WEB**, Versão 1.1 - 17/07/2020. Disponível em:

https://www.verifact.com.br/wp-content/uploads/2020/07/Parecer_Verifact_eSecurity-07-2020x.pdf. Acesso em 15 mar 2022.

FLORES, Daniel. A Cadeia de Custódia e a Ciência Forense Digital - CFD para a garantia da Autenticidade e Confiabilidade dos Documentos fontes de prova. **Palestra On-line TJDFT**. 38 slides, color, Padrão Slides Google Drive/Docs 4x3. Material elaborado para Palestra na Live Webinar Preservação Digital: o Case do TJDFT na Implementação do RDC-Arq. Brasília, DF. 03 de setembro de 2020. Disponível em: http://documentosdigitais.blogspot.com e em: http://abre.ai/bvSj Acesso em: 15 de abr. 2022.

FLORES, Daniel. Cadeia de custódia dos documentos arquivísticos digitais: do SIGAD ao RDC-Arq. Palestra. UFES. Vitória - ES. 76 slides, color, Padrão Slides Google Drive/Docs 4x3. Material elaborado para a Palestra no Curso de Arquivologia, 16 de junho de 2016. Disponível em: http://documentosdigitais. blogspot.com e em https://arquivologia.ufes.br/sites/arquivologia.ufes.br /files/field/anexo/cadeia_de_custodia_dos_documentos_arquivisticos_digitais-_do_sigad_ao_rdc-arq.pdf . Acesso em: 15 de abr. 2022.

FLORES, D.; ROCCO, B. C. B.; SANTOS, H. M. D. Cadeia de custódia para documentos arquivísticos digitais. **Acervo - Revista do Arquivo Nacional**, v. 29, n. 2, p. 117-132, 2016. Disponível em: http://hdl.handle.net/20.500.11959/brapci/40511. Acesso em: 15 abr. 2022.

GAGLIANO, Pablo Stolze, PAMPLONA FILHO, Rodolfo. **Manual de Direito Civil: volume único**. 3. ed., rev., ampl. e atual. São Paulo: Saraiva, 2019.

GONÇALVES, Victor Hugo Pereira. **O temerário uso da ata notarial para a formação de provas digitais**. Revista Consultor Jurídico, 2018. Disponível em: https://www.conjur.com.br/2018-jan-25/victor-goncalves-temerario-uso-ata-notarial-provas-digitais. Acesso em 15 mar 2022.

GRINOVER, Ada Pellegrini et. al. **Teoria geral do Processo**. 28ª ed. - São Paulo: Malheiros. 2012.

JORGE, Higor; JÚNIOR, Adair; GARZELLA, Oleno Carlos. **Manual de Interceptação Telefônica e Telemática - Teoria e Prática**. 1. ed. Salvador: Juspodivm, 2020.

LIMA, Renato Brasileiro de. **Manual de processo penal: volume único**. 8Ed – Salvador: JusPodivm, 2020.

LOPES JUNIOR, Aury. **Direito processual penal**. 16ª ed. São Paulo: Saraiva, 2019.

LOPES, Marilu; GABRIEL, Maria Madalena; BARETA, G. M. S. Cadeia de Custódia: uma abordagem preliminar. **Visão acadêmica**, v. 7, n. 1, 2006. Disponível em: https://revistas.ufpr.br/academica/article/view/9022/6315. Acesso em 15 abr 2022.

LUZ, Charlley; FLORES, Daniel. Cadeia de custódia e de preservação: autenticidade nas plataformas de gestão e preservação de documentos arquivísticos. **Seminário Serviços de Informação em Museus**, p. 171-181, 2018. Disponível em http://www .biblioteca.pinacoteca.org.br:9090/bases/biblioteca/322708.pdf. Acesso em 20 mar 2022.

MACHADO, Leonardo Marcondes. Aplicação da Cadeia de Custódia da Prova Digital. **Conjur**, 2020. Disponível em: https://www.conjur.com.br/2020-mar-31/academia-policia-aplicacao-cadeia-custodia-prova-digital#_ftn3. Acesso em: 05 abr. 2022

MARCACINI, Augusto Tavares Rosa. O documento eletrônico como meio de prova. Atual. **Augusto Marcacini**, 2006. Disponível em: http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico: Acesso em 15 mai. 2021.

MARQUES, Antônio Terêncio G. L. **A Prova Documental Na Internet**. 1. ed. 6ª reimpr. Curitiba: Juruá, 2011. 127p.

MEDEIROS, Gutembergue Silva; UGALDE, Júlio César Rodrigues. A ilegalidade da prisão baseada somente em reconhecimento fotográfico. **Conjur**, 2021. Disponível em: https://www.conjur.com.br/2021-mar-04/opiniao-prisao-baseada-reconhecimento-fotografico. Acesso em: 16 abr. 2022.

MONTEIRO, João. **Programa do Curso de Processo Civil**. 3. ed. São Paulo: Duprat, 1912, v. II, § 122, nota 2, p. 93.

MUNHOZ, Alexandre. *Blockchain* permite provas digitais confiáveis?. **Verifact**, 2021. Disponível em: https://www.verifact.com.br/blockchain-permite-provas-digitais-confiaveis/. Acesso em 19 mar 2022.

NETO, Mário Furlaneto; DOS SANTOS, José Eduardo Lourenço. APONTAMENTOS SOBRE A CADEIA DE CUSTÓDIA DA PROVA DIGITAL NO BRASIL. **Revista Em Tempo**, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. Acesso em: 15 abr. 2022. doi: https://doi.org/10.26729/et.v20i1.3130.

OLIVEIRA, Vinícius. ISO 27037 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. **Academia de forense digital**, 2019. Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/. Acesso em 19 mar 2022.

OLIVEIRA, Vinícius. A Cadeia de Custódia em Provas Digitais. **JusBrasil**, 2022. Disponível em: https://direitoetecnologia.jusbrasil.com.br/artigos/1335977844/a-cadeia-de-custodia-em-provas-digitais. Acesso em 19 mar 2022.

PONTES DE MIRANDA, Francisco Cavalcante. **Tratado de Direito Privado**. Tomo I, Parte geral. Campinas: Bookseeler, 2000.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. São Paulo: Marcial Pons, 2019.

PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. **Revista Consultor Jurídico**, 26 de janeiro de 2021. Disponível em: https://www.conjur.com.br/2021-jan-26/prado-notas-cadeia-custodia-prova-digital. Acesso em 15 de março de 2022.

REALE, M. **Lições Preliminares de Direito**, 25a ed. 22ª tiragem, São Paulo: Saraiva, 2001.

ROCHA, Jorge Bheron; TELES, Lara. Crimes Cibernéticos: Considerações Sobre a Criminalidade na Internet. **Âmbito Jurídico**, 2020. Disponível em: https://

ambitojuridico .com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes - sobre -a-criminalidade-na-internet/. Acesso em: 15 mar.2022.

SIPERCOM. **Parecer técnico**, **Versão 2.0 – 02/09/2019.** Disponível em: https://www.verifact.com.br/wp-content/uploads/2021/11/parecer-perito-v2.0-final-assinado.pdf. Acesso em: 18.03.2022.

SUZUKI E LOPES, Vicente Takaji e Hugo Fernando Men. **Verifact Parecer jurídico.** Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjjzoiwpND2AhWbILkGHSliBLYQFnoECAQQAQ&url=https%3A%2F%2Fwww.verifact.com.br%2Fwp-content%2Fuploads%2F2019%2F02%2Fverifact_parecer_juridico_v.2.1.pdf&usg=AOvVaw26ctzSkoWFbVgF6kUML5C_. Acesso em: 18.03.2022.

TEIXEIRA, Tarciso. **Curso de Direito e Processo Eletrônico: Doutrina, Jurisprudência e Prática** – 3. ed. atual. e ampl. – São Paulo: Saraiva, 2015.

THEODORO JÚNIOR, Humberto. **Curso de Direito Processual Civil. Teoria geral do direito processual civil, processo de conhecimento e procedimento comum**. Volume I. 56ª edição. Rev., atual. e ampl. Rio de Janeiro. Editora Forense, 2015.

VERIFACT. Registros de provas digitais, c2022. Colete provas digitais auditáveis e com validade jurídica. Disponível em: https://www.verifact.com.br/. Acesso em: 15.03.2022.