UNIVERSIDADE REGIONAL INTEGRADA DO ALTO URUGUAI E DAS MISSÕES
PRÓ-REITORIA DE ENSINO, PESQUISA E PÓS-GRADUAÇÃO
CÂMPUS DE ERECHIM
DEPARTAMENTO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

GABRIELA SOMENZI

A CADEIA DE CUSTÓDIA DA PROVA PENAL DIGITAL: uma análise das etapas e desafios para sua preservação

ERECHIM
2023

GABRIELA SOMENZI

A CADEIA DE CUSTÓDIA DA PROVA PENAL DIGITAL: uma análise das etapas e desafios para sua preservação

Trabalho apresentado ao Curso de Direito do Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões (URI) – Erechim/RS, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. M.e. Andrey Henrique Andreolla.

ERECHIM

2023

GABRIELA SOMENZI

A CADEIA DE CUSTÓDIA DA PROVA PENAL DIGITAL: uma análise das etapas e desafios para sua preservação

Trabalho de conclusão de curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito, pelo Curso de Direito do Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões.

Erechim/RS, ___ de _____ de 2023.

BANCA EXAMINADORA

_____

(Nome do orientador, titulação e Instituição a que pertence).

_____

(nome, titulação e instituição a que pertence).

_____

(nome, titulação e instituição a que pertence).

AGRADECIMENTOS

Em primeiro lugar, gostaria de expressar minha profunda gratidão aos meus pais, cujo apoio e orientação foram fundamentais para eu manter minha resiliência durante essa jornada e concluir este projeto. Também sou grata aos meus irmãos, que têm sido verdadeiras fontes de inspiração em minha vida, desempenhando um papel crucial em meu progresso até agora.

Quero também agradecer, em especial, o meu namorado Leonardo, pois sem ele, esta jornada teria sido ainda mais desafiadora. Agradeço sinceramente pela paciência que teve comigo durante este período e pelo apoio incondicional, especialmente no aspecto emocional, vez que sempre fez questão de me tranquilizar e me motivar, permitindo que eu chegasse até aqui.

Além disso, expresso meu agradecimento ao meu orientador, Mestre Andrey Henrique Andreolla, por toda a assistência, dedicação e tempo investido, tendo desempenhado papel fundamental na produção e conclusão deste trabalho. Gostaria também de enfatizar a honra que foi para mim trabalhar sob sua orientação, pois não é apenas um excelente educador, mas também um advogado e pesquisador excepcional.

Por fim, agradeço a todos que de alguma forma contribuíram ao longo desta jornada, todos meus amigos, em especial as minhas colegas Laísa, Andressa, Zidiani e Tariane, meus familiares, professores e a Instituição de Ensino URI-Erechim.

RESUMO

Tendo em vista a grande incidência de provas digitais durante a persecução penal, em decorrência da sociedade informatizada, pesquisa-se sobre a cadeia de custódia da prova digital. Objetiva-se de responder quais são as etapas, bem como quais são os principais problemas e desafios para sua preservação. Objetivando responder este impasse, é necessário, primeiramente, compreender o contexto atual da sociedade e seu impacto no direito penal e processual penal, em seguida, conhecer os principais aspectos da prova digital e, ao final, analisar quais são as etapas da cadeia de custódia da prova digital e os principais problemas e desafios hodiernos em relação a tal procedimento. Realiza-se, então, uma pesquisa bibliográfica, utilizando-se do método indutivo analítico-descritivo. Diante disso, como resultado da pesquisa, verifica-se que inexiste lei específica e concreta que defina quais são as etapas da cadeia de custódia da prova digital. Só foi possível responder à pergunta do presente trabalho por meio de uma análise conjunta da doutrina, da jurisprudência e da ABNT NBR ISO/IEC 27037 2013. Ainda, quanto a referida norma técnica, trata-se da única previsão normativa quanto a cadeia de custódia da prova digital. Contudo, além de ser antiga, não prevê exatamente as etapas, mas apenas o procedimento do manuseio inicial da evidência digital. Como resultado, verificou-se a existência de vários empecilhos, não só em relação a falta de legislação, mas também a falta de preparo técnico dos profissionais, investimento nas instituições e a falta de previsão legal sobre os motivos que ocasionam a quebra da cadeia de custódia deste tipo de prova, e os seus efeitos. Ante o exposto, conclui-se pela necessidade de edição de lei específica quanto a matéria, prevendo as etapas, quando ocorre a quebra e quais os efeitos desta, bem como a implementação de políticas para aperfeiçoamento dos órgãos e capacitação dos profissionais que detenham a função de atuar na persecução penal, tudo para garantir decisões mais próximas da verdade real, evitando-se, assim, erros judiciários e injustiças.

Palavras-chave: cadeia de custódia; direito digital; processo penal; prova; tecnologia.

ABSTRACT

Considering the high incidence of digital evidence during criminal prosecution, as a result of the computerized society in which we operate, research the chain of custody of digital evidence, in order to answer what the steps are, as well as what the main problems are. and challenges for its preservation. In order to respond to this impasse, it is necessary, firstly, to understand the current context of society and its impact on criminal law and criminal procedure, then, to know the main aspects of digital evidence and, in the end, to analyze the stages of the chain of custody. of digital proof and the main current problems and challenges in relation to this act. A bibliographical research is then carried out, using the inductive analytical-descriptive method. Therefore, as a result of the research, it appears that there is no specific and concrete law that defines the stages of the digital evidence chain of custody. It was only possible to answer the question of this work through a joint analysis of doctrine, jurisprudence and ABNT NBR ISO/IEC 27037 2013. Furthermore, regarding the aforementioned technical standard, it is the only normative provision regarding the chain of custody of digital evidence, however, in addition to being old, it does not provide exactly the steps, but rather only the procedure for the initial handling of digital evidence. Also as a result, the existence of several obstacles was verified, not only in relation to the lack of legislation, but also the lack of technical preparation of professionals and also the lack of legal provision regarding the reasons that cause the chain of custody of this item to be broken. type of evidence, and its effects, with there being little discussion in jurisprudence on this topic. In view of the above, it is concluded that there is a need to issue a specific law on the matter, predicting the stages, when the breach occurs and what its effects are, as well as the implementation of policies to improve bodies and train professionals, who hold the function of acting in criminal prosecution, all to guarantee decisions that are as close as possible to the real truth, thus avoiding judicial errors and injustices.

Key words: chain of custody; digital law; criminal proceedings; proof; technology.

SUMÁRIO

1 INTRODUÇÃO

Na sociedade da informação em que se vive, impulsionada pelo progresso tecnológico e principalmente pela internet, é cada vez mais frequente o uso de dispositivos eletrônicos e o acesso à rede. Isso é evidenciado pelos resultados da pesquisa realizada pelo IBGE em 2019, que revelou um aumento significativo no uso da internet pelos brasileiros, passando de 74,7% em 2018 para 78,3% em 2019, sendo que a principal atividade online foi o envio de mensagens (IBGE, 2019). Além disso, dados da 33ª pesquisa anual sobre o uso de tecnologia da informação pela FGVcia (2022), mostraram um notável aumento no número de dispositivos conectados à internet no Brasil em 2021, totalizando 424 milhões, em comparação com uma população de 213 milhões no mesmo ano.

Tais avanços impactam diretamente o direito, inclusive na área criminal. Não só quanto a prática de crimes cibernéticos, mas, também, quanto a produção de provas digitais, afinal, à medida que mais se utiliza de dispositivos eletrônicos e da internet, a atividade digital aumenta, gerando, por consequência, à produção de evidências digitais.

Diante o exposto, considerando a grande incidência da prova digital no processo penal, surge a preocupação quanto a preservação de sua autenticidade e integridade. Para tanto, a Lei 13.964/2019 (Lei Anticrime), instituiu a cadeia de custódia, a qual tem a finalidade de garantir a lisura e a validade da prova. Entretanto, a cadeia de custódia positivada no Código de Processo Penal não faz menção sobre quais são as etapas a serem observadas quando se tratar de prova digital. Nesta perspectiva, nota-se a necessidade de conhecer quais são as etapas da cadeia de custódia desta espécie de prova. Diante disso, indaga-se: quais são as etapas da cadeia de custódia da prova penal digital e os obstáculos a serem superados para sua preservação?

A necessidade de responder a essa pergunta, justifica-se pelo aumento das evidências digitais, tornando-se essencial entender como manejar adequadamente esse tipo de prova, afinal, trata-se de material probatório extremamente volátil, o que significa fácil alteração e perda. Portanto, é essencial manter a integridade da cadeia de custódia da prova digital para garantir o devido processo legal. A ignorância quanto as etapas a serem seguidas pode gerar a quebra da cadeia de custódia, prejudicando tanto as partes do processo, quanto a sociedade em geral. Desrespeitar a cadeia de

custódia da prova digital, pode ocasionar em impunidades por falta de provas, quando ela torna-se inutilizável, ou até mesmo ocasionar injustiças, caso sua autenticidade não seja verificada corretamente.

Sendo assim, o objetivo geral da presente pesquisa é entender quais são as etapas, bem como os principais problemas e desafios relacionados à cadeia de custódia da prova digital. Para tanto, foram delineados os seguintes objetivos específicos: entender o atual momento da sociedade, a partir do conceito de sociedade da informação e a quarta revolução industrial, e a sua ligação com a criminalidade virtual e as provas digitais; compreender a prova digital e seus meios de obtenção e produção; e analisar as etapas da cadeia de custódia da prova digital e os principais problemas e desafios hodiernos em relação a tal ato.

Parte-se da hipótese de que a legislação penal brasileira não prevê normas que estabeleçam quais são as etapas da cadeia de custódia da prova digital, nem mesmo quando ocorre e quais os efeitos da sua quebra. Além disso, a falta de lei não é o único impasse, vez que a falta de estrutura das organizações e treinamento técnico das pessoas envolvidas na persecução penal, também são um empecilho. Assim, a fim de viabilizar esta hipótese, realiza-se uma pesquisa bibliográfica, utilizando como método de abordagem, o indutivo, e como método de procedimento, o analítico descritivo.

No primeiro capítulo, é realizada uma análise do cenário atual da sociedade, focando na revolução 4.0 e na sociedade da informação, bem como o impacto dessa tecnologia no direito penal e processual penal, incluindo os cibercrimes e investigações virtuais. O segundo capítulo aborda a prova digital, começando com a teoria geral da prova, e, em seguida, com o estudo sobre o conceito, características, classificação, natureza jurídica, meios de obtenção e produção da prova digital. Finalmente, o terceiro capítulo traz uma análise geral da cadeia de custódia, e após, por meio da análise da doutrina e da jurisprudência, traz as etapas da cadeia de custódia da prova digital, a sua quebra e os obstáculos em relação a esta temática.

Ao final, conclui-se que os objetivos são atingidos e a pergunta resta respondida, com a confirmação da hipótese. Se faz necessária previsão legislativa específica quanto a cadeia de custódia da prova digital, vez que as etapas e sua quebra são previstas de forma única e limitada, apenas na doutrina e jurisprudência, o que põem em risco o devido processo legal e a busca pela decisão mais próxima à verdade real.

2 A REVOLUÇÃO 4.0 E A SOCIEDADE DA INFORMAÇÃO: IMPACTOS NA ÁREA DO DIREITO PENAL E PROCESSUAL PENAL

A cadeia de custódia é um importante instrumento de preservação da prova penal, a qual ganhou grande ênfase com o advento da Lei 13.964/19 (Lei Anticrime), bem como pela sua inserção no Código de Processo Penal Brasileiro, no ano de 2020. Todavia, com a sociedade da informação vivenciada nos tempos atuais, marcada pela internet, pelos algoritmos, pelo ciberespaço e outras tantas tecnologias avançadas, a cadeia de custódia deve se adequar à prova que vem ganhando cada vez mais espaço, qual seja, a prova digital. Diante disso, inicialmente, faz-se necessário entender o atual momento da sociedade para compreender a relevância de tal temática.

2.1 RELEVÂNCIA DO TEMA

De acordo com a obra Futuro Presente, Guy-Perelmuter (2019) destaca que atualmente vivencia-se uma nova etapa de progresso científico, no qual se popularizou a utilização de elementos tecnológicos que se tornaram comuns no dia a dia das pessoas, tais como computadores, celulares, internet, inteligência artificial, nanotecnologia e os armazenamentos ilimitados de dados. Diante disso, o autor questiona sobre como a sociedade se adequará a tais mudanças, já que estas impactarão todas as esferas da sociedade.

Para que se possa demonstrar a magnitude do afirmado acima, a 33ª pesquisa anual do uso de TI da FGVcia (2022), apontou que a população Brasileira no ano de 2016 era de 206 milhões de habitantes, sendo que os dispositivos conectados à internet totalizavam 244 milhões. Já em 2021, a população teve pequeno crescimento de 213 milhões de habitantes, e, por outro lado, expressivo aumento de dispositivos conectados à internet, somando 424 milhões, ou seja, um aumento de 180 milhões de dispositivos conectados à rede mundial de computadores, no período de 05 anos.

Em vista disso, é natural que a nova realidade social impacte as mais diversas áreas, inclusive a do direito, já que este tem “a missão de regular as relações sociais, e, sendo estas últimas cada vez mais virtuais ou digitais, é imperioso que as normas jurídicas acompanhem tal mudança” (Miziara, 2022, não paginado). Sendo assim, os métodos jurídicos tradicionais tornam-se insuficientes, tanto na área do direito material

quanto no direito processual, devendo, portanto, se adequar a atual sociedade (Miziara, 2022).

Dentre estas mudanças em que o direito deve buscar adequação, destaca-se a prova penal digital, objeto do presente estudo, a qual vem ganhando grande espaço dentro da persecução penal, já que:

> quanto maior o número de dispositivos conectáveis à internet, maior será a atividade digital das pessoas. Quanto maior a atividade digital, mais fatos sociais ocorrerão em ambiente virtual. E, se há um aumento dos fatos que acontecem em ambiente virtual, é natural que os meios de provas digitais ganhem destaque e importância. Isso se dá porque na maioria dos casos, embora isso nem sempre ocorra, os fatos ocorridos em ambiente virtual são demonstrados por meios de provas digitais (Miziara, 2022, não paginado).

No entanto, no âmbito legislativo, não há regras que possam apresentar solução jurídica para este problema, já que inexistem normas que disciplinam a classificação, procedimento, valor probatório e a cadeia de custódia de uma prova digital (Vaz, 2012). Além disso, o Projeto de Lei 8.045/2010, que trata do novo Código de Processo Penal, também não faz menção a tal assunto (Vaz, 2012).

Sendo assim, é importante compreender a evolução da sociedade, através das revoluções industriais e a sociedade da informação, bem como os novos instrumentos tecnológicos e os impactos disso no direito penal e processual penal, tais como o cibercrime e as investigações digitais, para compreender a importância de conhecer quais são as etapas da cadeia de custódia de uma prova penal digital e os desafios a serem enfrentados para evitar sua quebra, buscando maior proteção.

2.2 AS QUATRO REVOLUÇÕES INDUSTRIAIS E OS AVANÇOS TECNOLÓGICOS ATÉ A ERA DA INFORMATIZAÇÃO

Desde os primórdios, a sociedade está em constate desenvolvimento, tendo passado por diversas revoluções, as quais deram causa a mudanças abruptas e radicais em nossa sociedade, tanto na sua estrutura econômica quanto social, sendo que a primeira delas ocorreu a mais de 10.000 mil anos atrás, com a revolução agrícola, época em que se utilizou a domesticação de animais, levando ao surgimento das primeiras cidades e da urbanização (Schwab, 2016).

Já a partir da metade do século XVIII, surgiram as grandes revoluções industriais, que tiveram marco histórico com a substituição da força física pela

utilização de máquinas (Schwab, 2016). Para Hobsmawm (2000), a revolução industrial foi a transformação mais radical da humanidade, pois proporcionou a aceleração do crescimento econômico e das mudanças sociais.

Quanto à Primeira Revolução Industrial, esta teve início em 1760, na Inglaterra, em que o aumento da população, a migração do campo para a cidade e os avanços científicos, deram causa ao início da industrialização e das inovações, como a máquina a vapor (Cavalcanti; Silva, 2011). Além disso, a revolução caracterizou-se pela substituição da mão de obra humana pelas máquinas, ou seja, substituiu-se a produção manufatureira pela maquinofatura, sendo que o setor têxtil foi o primeiro a fazer o uso dessa inovação (Iglésias, 1990).

A partir da metade do século XIX, entre os anos de 1850 a 1870, surgiu a Segunda Revolução Industrial, a qual perdurou até a Segunda Guerra Mundial. Diferente da Primeira Revolução, a Segunda atingiu outros países além da Inglaterra, tais como a Itália, Alemanha, França, Japão, Estados Unidos e Rússia (Lopes; Garcias; Assumpção, 2020).

Nesta revolução, deixou-se de fabricar motores e máquinas simplificadas e passou-se a criar grandes maravilhas mecânicas, tais como o trem, capaz de se locomover a 20 km por hora (Lopes; Garcias; Assumpção, 2020). Ademais, a partir de 1873, a energia elétrica começou a ser utilizada na indústria, dando origem aos motores elétricos, e assim, a fonte de energia deixou de ser o vapor, sendo substituído pelo petróleo e pela eletricidade (Lopes; Garcias; Assumpção, 2020).

Além disso, durante a Segunda Guerra Mundial, surgiram grandes avanços na área da ciência, e foi durante este período, no ano de 1940, que o computador foi criado (Vaz, 2012). Inicialmente, eles serviam apenas para propósito militar, no entanto, a partir da década de 50 e 60, os computadores atingiram maior velocidade e começaram a ser comercializados (Vaz, 2012).

Diante deste contexto, é que se originou a Terceira Revolução Industrial, no século XX, com início na década de 1960, que também ficou conhecida como a revolução digital ou a revolução do computador (Schwab, 2016). Foi durante este período, especificamente entre a década de 70 e 80, que, graças ao microprocessamento, o computador diminui seu tamanho e aumentou sua velocidade, motivo pelo qual passou a ser utilizado amplamente pela sociedade, tanto no âmbito profissional, quanto educacional e até familiar (Vaz, 2012).

No ano de 1968 também foi criada a internet, que apesar de ter nascido com propósito de auxiliar as forças militares, evoluiu assim como o computador, e em 1990, passou a ser amplamente utilizada pela população (Vaz, 2012). Como se não bastasse isso, também foram criados outros famosos dispositivos eletrônicos, tais como o celular, GPS, mp3, câmeras digitais, entre outros (Vaz, 2012).

> Houve, assim, a substituição, em grande medida, de meios tradicionais de expressão por novos meios tecnológicos. Apenas como ilustração, pode-se citar que: os documentos anteriormente redigidos e arquivados em papel tornaram-se eletrônicos; as músicas foram transferidas do disco de vinil e da fita cassete para o formato digital; as fotografias deixaram de ser registradas em filme para também assumirem o formato digital; do mesmo modo, a captação de imagens em vídeos; e ainda a comunicação por cartas, bilhetes, telegrama, telefone, foi transmudada em mensagens eletrônicas de texto, e-mails, sistemas VoIP, dentre outros (Vaz, 2012, p. 7).

Diante deste cenário, verifica-se que já na Terceira Revolução Industrial, a criação e armazenamento de informações se dava em formato digital. Sendo assim, a partir desta época, os dispositivos eletrônicos foram se aperfeiçoando, e a sociedade passou a ser cada vez mais adepta ao meio digital.

Graças a isso, o alemão Klaus Schwab (2016) entende que a partir do início do século XXI, os *softwares*, computadores e redes estão se tornando cada vez mais aprimorados, gerando dessa forma uma ruptura com a Terceira Revolução Industrial. Diante disso, Schwab (2016) considera que hoje vivencia-se a Quarta Revolução Industrial ou também conhecida como a Indústria 4.0.

> A quarta revolução industrial, no entanto, não diz respeito a apenas sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de novas descobertas ocorrem em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis a computação quântica, o que torna a quarta revolução industrial fundamentadamente diferente das anteriores é a fusão desta tecnologia com e a interação entre os domínios físicos, digitais e biológicos (Schwab, 2016, p. 16-17).

Enquanto a Primeira Revolução Industrial foi marcada pela energia a vapor e as primeiras máquinas, a Segunda pelo aperfeiçoamento destas e da utilização do petróleo e da eletricidade como fonte de energia e, a Terceira pela invenção do computador, da internet e de outros dispositivos eletrônicos, a Quarta Revolução Industrial surgiu como um aperfeiçoamento de todas essas tecnologias já inventadas.

Isso porque, a Revolução 4.0 é caracterizada pela difusão da internet, de sensores menores e mais poderosos, bem como pela inteligência artificial (Schwab, 2016). Além disso, este fenômeno também é marcado pelo sistema de produção Ciber-Físicos, o qual possibilita que as máquinas não precisem mais ser monitoradas pelo homem, utilizando-se de sensores para determinar quando elas devem avançar e quando parar (Lopes; Garcias; Assumpção, 2020).

Para Schwab (2016), tal evolução foi possível graças a três fatores. O primeiro deles é a velocidade, ao entender que esta revolução se deu de forma mais rápida que as demais, graças a globalização e o fato de a tecnologia gerar mais tecnologia. O segundo fator é a amplitude e diversidade, uma vez que a evolução digital se trata de uma combinação de diversas tecnologias, gerando mudanças em todas as áreas da sociedade e, principalmente, no próprio indivíduo. Por fim, o terceiro fator refere-se ao impacto sistêmico, ao entender que a Quarta Revolução influência e transforma tudo o que ela atinge.

Nesta conjuntura, com a disseminação deste mundo virtual, com maior velocidade e menor custo, é natural que as pessoas passem a se adaptar a este novo modelo de vida, inclusive, não se trata mais de uma opção, mas sim de uma necessidade das pessoas (Soares, 2018). Sendo assim, as ações realizadas no cotidiano estão tornando-se cada vez mais digitais, tendo em vista que a produção, aquisição, armazenamento e distribuição de informações se dão por meios eletrônicos e virtuais (Minto, 2021).

Por este motivo, é que para Castells (2002, p. 68), “o cerne da transformação que estamos vivendo na revolução atual, refere-se à tecnologia da informação, processamento e comunicação”. Ou seja, a informação é o elemento principal da Quarta Revolução Industrial, tendo em vista que graças ao aprimoramento da internet, aquela pode ser acessada e compartilhada de forma imediata por qualquer pessoa, gerando desta forma uma ampla globalização e valorização do meio digital.

2.3 A SOCIEDADE DA INFORMAÇÃO

A partir da metade do século XX, com a criação do computador, da internet, e outros diversos dispositivos eletrônicos, a sociedade passou por uma transformação que deu causa a revolução informacional, e com ela, surgiu o fenômeno da sociedade da informação (Vaz, 2012). Desde então, para Werthein (2000), as indústrias deixaram

de ser o fator principal, dando espaço para a era da telecomunicação e da microeletrônica. Para compreensão deste novo modelo de sociedade, Castells (2002, p. 69) entende que:

> o que caracteriza a atual revolução tecnológica não é a centralidade de conhecimento e informação, mas a ampliação desse conhecimento e dessa informação para a geração de conhecimento e de dispositivo de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso.

Assim, a sociedade da informação se caracteriza pelo compartilhamento de informações a uma escala global, e não mais centralizada, possibilitando que todos conectem-se ao mesmo tempo e tenham acesso aos mesmos conteúdos. Por conseguinte, os meios de criação, armazenamento e propagação dessas informações passam por atualizações constantes, e assim, novas tecnologias são criadas, principalmente no campo digital. Neste sentido, Gouveia (2004, não paginado), destaca as proporções que este fenômeno pode atingir:

> a sociedade da informação está inserida num processo pelo qual a noção de espaço e tempo tradicional estão em transformação pelo surgimento de um “espaço virtual”, transterritorial, transtemporal, que formará uma telecidade, numa tele-sociedade que se sobreporará mesmo aos Estados clássicos, criando novas formas de inter relações humanas e sociais, ainda que por vezes ocorram conflitos neste processo de transformação.

A aposta feita pelo autor se realizou, tendo em vista que, de acordo com informações disponibilizadas pelo site G1, em dezembro de 2021, baseada em dados da Organização das Nações Unidas (ONU) e da União Internacional de Telecomunicações (UIT), cerca de 4,9 bilhões de pessoas estão conectadas à internet, sendo que em 2021 foi verificado um aumento de aproximadamente 800 milhões de usuários em decorrência da Pandemia da Covid-19 (Presse, 2021).

Dentre os diversos usos da internet, pode-se destacar a utilização de redes sociais, como o Facebook, o Instagram, o WhatsApp, e, mais recentemente, o TikTok. Segundo dados divulgados no Portal O Globo, em 2022, o número de usuários do Instagram ultrapassou os 2 bilhões, aproximando-se dos 2,96 bilhões de usuários do Facebook (O Globo, 2022). Já o TikTok possui mais de 1 bilhão de usuários, tendo se popularizado no Brasil durante a Pandemia causada pelo coronavírus (Dean, 2022). Por sua vez, o WhatsApp possui mais de 2 bilhões de usuários no mundo (Dean,

2022). Esses números demonstram o acerto da previsão feita por Javier em 2004, pois quase 5 bilhões de pessoas estão conectadas à internet, enquanto, somente nas plataformas acima citadas, o número de usuários ultrapassa os 7 bilhões.

Além disso, o acesso à internet de mais de 2/3 da população do planeta permite que grande parte das pessoas tenham acesso à informação, fatos e acontecimentos atuais envolvendo qualquer parte do globo. Portanto, sem dúvidas a sociedade sofreu grande transformação nos últimos anos, tornado-se uma tele-sociedade, isto é, uma sociedade que está conectada por meio de aparelhos com acesso à internet, fazendo uso de diversos aplicativos e sites, adquirindo informações e se interrelacionando em tempo real.

Em decorrência das relações e facilidades advindas do uso da internet e dos equipamentos eletrônicos, é natural que se produzam grande número de dados, caracterizados por fotos, vídeos, mensagens, troca de e-mails, notícias, entre outros. Como prova disso, destaca-se a pesquisa feita por Bernardo Viana (2021, não paginado), a qual aponta que em 350 anos o número de dados produzidos pela humanidade ultrapassará o número de átomos existentes no mundo, e que até 2025 serão produzidos 175 zettbytes de dados, equivalente a 175 trilhões de gigabytes.

A produção de tamanha quantidade de dados acaba por ter implicação direta no direito, principalmente no tocante ao direito penal e processual penal, tendo em vista que o uso da rede, apesar dos benefícios, também ocasionou a inovação na forma de praticar crimes (virtuais ou não), bem como de produzir, ocultar e armazenar provas relacionadas a estes delitos. Portanto, antes de adentrar no tema principal deste trabalho, é necessário entender o conceito e as funcionalidades de alguns dos dispositivos eletrônicos mais utilizados nesta era digital.

2.4 DISPOSITIVOS ELETRÔNICOS E AS NOVAS FORMAS DE OBTENÇÃO E ARMAZENAMENTO DE DADOS

Entender quais são os dispositivos eletrônicos e sistemas informáticos, bem como quais são suas funcionalidades, é fundamental para compreender como as informações são criadas, compartilhadas e armazenadas, pois é a partir disso que nascem as provas digitais.

2.4.1 Computadores e seus componentes

A criação do computador foi o marco das inovações tecnológicas digitais que se vive hodiernamente. Tal equipamento teve origem no século XIX e inicialmente foi criado com objetivo de auxiliar nos cálculos, por este motivo é que a palavra computador tem origem do latim *computare*, que significa calcular ou contar (Vaz, 2012).

Quanto à sua conceituação, Pinheiro (2010, p. 55) entende que “o computador é uma máquina composta de elementos físicos do tipo eletrônico, capaz de realizar grande variedade de trabalhos com alta velocidade e precisão, desde que receba as instruções adequadas”. Além disso, Cunha, Macedo e Silveira (2017, p. 14) entendem que o computador:

> permite que a maioria das tarefas complexas sejam executadas em um tempo infinitamente menor que se fossem executadas pelo homem. Dessa forma, o computador é um dispositivo que aumenta significativamente a variedade de tarefas e atividades que podem ser desenvolvidas pelo ser humano.

Ademais, quanto à sua estrutura, o computador é uma máquina com vários componentes eletrônicos, os quais devem estar conectados a eletricidade. Entre eles, destaca-se os hardwares e os softwares (Cunha; Macedo; Silveira, 2017). Primeiramente, quanto aos hardwares, estes são os componentes físicos do computador, que podem ser externos ou internos (Vaz, 2012). Além disso, cada hardware é individualizado e identificado pela função que exerce, como por exemplo o teclado, o qual tem a finalidade de digitar textos (Cunha; Macedo; Silveira, 2017).

Os principais componentes do hardware são os microprocessadores e a memória. Quanto ao primeiro, também conhecido como unidade central de processamento (CPU), “representa o cérebro do computador, realizando as funções aritméticas, lógicas e de controle” (Vaz, 2012, p. 10).

Já o segundo componente, a memória, são todos os dispositivos responsáveis por armazenar dados, de forma temporária ou permanente. Dentre estes dispositivos, existem a memória RAM e a memória ROM (Cunha; Macedo; Silveira, 2017).

A primeira delas é a memória de trabalho do computador, a qual possibilita que este consiga realizar suas operações, além disso, caracteriza-se pela sua volatilidade, pois as informações se perdem quando o computador é desligado. Já a

segunda, é responsável por guardar códigos básicos de operação do equipamento, permitindo apenas a leitura das informações, não podendo estas serem alteradas, além de que não se perdem com o desligamento do aparelho (Cunha; Macedo; Silveira, 2017).

Por outro lado, os softwares são um conjunto de instruções, conhecidos como programas, utilizados para permitir que os hardwares executem suas tarefas. Eles são divididos em duas categorias, os softwares básicos e os softwares aplicativos (Cunha; Macedo; Silveira, 2017).

O software básico é responsável por auxiliar a execução dos softwares aplicativos. Além disso, um dos seus principais componentes é o sistema operacional, responsável pela interação entre hardwares e usuários/ou softwares aplicativos, como por exemplo o Windows. Já o software aplicativo, serve para executar operações de interesse dos usuários, tais como pacotes de escritório (Office) ou programas para conectar as pessoas às redes sociais (Cunha; Macedo; Silveira, 2017).

2.4.2 A internet das coisas

O nome internet advém de duas palavras do inglês, *international network*, que traduzidas para o português significam rede internacional. Logo, a internet nada mais é que uma rede mundial de computadores interligados, por meio dos quais são produzidas e transmitidas as informações a qualquer usuário que esteja conectado (Mota, 2010). Já para Cunha e Cavalcanti (2008, p. 212), a Internet é a “união de várias redes de teleprocessamento estaduais, regionais, nacionais e internacionais – em uma lógica, compartilhando um mesmo esquema de endereçamento”.

O seu surgimento se deu durante a guerra fria, quando em 1957 os russos lançaram o *Sputinik*[1], fazendo com que os Americanos se mobilizassem para criar um sistema que facilitasse a troca de informações, com objetivo de evitar ataques soviéticos (Eduvirges; Santos, 2013). Assim, em 1969, a DARPA[2] criou uma rede de computadores chamada ARPANET[3], a qual ligava quatro universidades americanas,

[1] Primeiro satélite artificial produzido pelo programa soviético.
[2] Departamento de Defesa dos Estados Unidos.
[3] Advanced Research Projects Agency Network. Tradução: Rede de agências para projetos de pesquisas avançadas.

permitindo que cientistas se comunicassem e trocassem informações em longa distância (Mota; 2010).

Diante disso, nota-se que inicialmente a internet nasceu apenas com propósitos militares. Porém, a partir da década de 90, esta passou a ser utilizada amplamente pelas pessoas, não se limitando mais a fins militares ou acadêmicos (Eduvirges; Santos, 2013). A partir de então, “a Internet cresceu rapidamente como uma rede global de redes de computadores” (Castells, 2002. pág. 15).

Já no ano de 1999, nasceu o termo Internet das Coisas, pelo pesquisador britânico Kevin Ashton (Ferreira *et al*., 2021). Para Dias (2016), a internet das coisas é a conexão entre o mundo real e o mundo virtual. Ainda, para Colombo e Lucca Filho (2018), trata-se da conexão de qualquer objeto físico à rede de internet.

Além disso, para melhor compreensão de tal termo, Koreshoff, Robertson e Leong (2013), entendem que coisa é todo objeto, lugar ou ambiente do nosso cotidiano. Ademais, Fleisch (2010) entende que todas as coisas físicas do mundo podem ter características de pequenos computadores, e assim, todas elas poderão se conectar à internet e se tornarem objetos inteligentes.

Ou seja, a conexão à internet não se limita mais a apenas computadores tradicionais, mas sim a qualquer coisa física móvel, como os smartphones, os automóveis e, até mesmo, utensílios de limpeza de uma casa, como um aspirador de pó inteligente. Além disso, a internet das coisas possibilita que esses objetos se conectem uns aos outros, como por exemplo, quando o celular é conectado no rádio do carro para compartilhar uma música, ou até mesmo um comando dado pelo celular a um eletrodoméstico.

2.4.3 As novas formas de criação, transmissão e armazenamento de informações e a produção de dados digitais

Com a criação do computador e da internet, bem como pela fusão destes, a criação, transmissão e arquivamento de informações passam a ser cada vez mais digitais. Diante disso, neste momento serão analisados alguns dos mecanismos de informação mais utilizados e quais suas finalidades.

Um dos principais meios de obtenção e transmissão de informações utilizados hoje é a Web, termo simplificado de *World Wide Web*. Trata-se de uma ferramenta de acesso à internet, composta por um conjunto de sites e que possibilita o acesso a

dados/informações hospedadas em outros computadores (Magrini, 2018). Para melhor compreensão, o internauta, por meio da utilização de um browser (navegadores como Internet Explorer e Chrome), acessa estes sites, que nada mais são do que páginas na internet, e dessa forma, conseguem encontrar diversos arquivos e informações em forma de textos, músicas, sons e imagens (Vaz, 2012).

Além disso, destacam-se outras formas de transmissão de informações, tais como o e-mail, aplicativos e o sistema VoIP. O e-mail é uma forma de correspondência eletrônica, composta por um endereço de envio e outro de destino, capaz de transmitir textos, imagens e vídeos (Vaz, 2012). Já o sistema VoIP é uma tecnologia capaz de "transmissão da voz por pacotes de dados, ligando telefones e computadores" (Vaz, 2012, p. 28).

Ainda, os aplicativos tratam-se de softwares/programas inteligentes que possuem a finalidade de facilitar a utilização de um hardware, tais como a calculadora e o Word, além da finalidade de entretenimento e acesso a informações, como o WhatsApp e o TikTok (Boniati; Preuss e Franciscatto, 2014).

Também se destacam as novas formas de armazenamento dessas informações, como em nuvem, o qual, segundo a Amazon Web Services (2020), é um modelo de computação que permite armazenar grande quantidade de dados em um provedor de computação em nuvem acessível por meio da internet, ou seja, fora do sistema de armazenamento do dispositivo do usuário.

Em suma, a utilização destes dispositivos ocasionou uma enorme criação e armazenamento de dados digitais. Segundo Magrani (2018, p. 22), estima-se que "nos próximos anos, a medida em gigabytes[4] será superada e o cálculo da quantidade de dados será feito na ordem zettabyte[5] e até em yottabyte[6]".

Logo, naturalmente que o aumento do uso da internet e o acesso aos dispositivos eletrônicos a ela conectados, facilitou, modificou e ampliou as formas de transmissão, criação e obtenção de dados digitais e de informações. Por consequência disso, o ramo do direito penal e processual penal sofre implicações, tanto na prática de crimes, quanto nas investigações criminais.

[4]Gigabyte é uma unidade de medida de informação que equivale a 1 trilhão de bytes.
[5]Zettabyte é uma unidade de informação que corresponde a 1 sextilhão de bytes.
[6]Yottabyte é uma unidade de medida de informação que equivale a 10^{24} bytes.

2.5 A INFLUÊNCIA DA ERA TECNOLÓGICA DIGITAL NO DIREITO PENAL E PROCESSUAL PENAL E AS PROBLEMÁTICAS ATUAIS

Por ser o direito reflexo do que acontece na sociedade, por óbvio que esta era tecnológica e digital geraria impactos na área. Assim, neste momento serão analisadas algumas das problemáticas atuais enfrentadas no direito penal e processual penal, em decorrência desta era da informatização e virtualização.

2.5.1 Criminalidade virtual

Apesar da tecnologia digital trazer diversos benefícios à sociedade, o meio virtual também se tornou palco da prática de crimes, popularmente conhecidos por cibercrimes ou crimes informáticos/cibernéticos. Para Lorenzo e Scaravelli (2021), os cibercrimes tratam-se de delitos cometidos em espaços fictícios, tais como a internet, computadores ou outros dispositivos eletrônicos, não sendo necessário abordar a vítima fisicamente/presencialmente. Ainda, para Rosa (2002, p. 53) crime cibernético é “toda ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento automático de dados ou transmissão”. Além disso, importante destacar que a conduta não precisa obrigatoriamente ser cometida na internet, basta que ocorra em qualquer sistema informático.

> A denominação “delitos informáticos” alcança não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta sem imprescindível “conexão” à Rede Mundial de Computadores, ou qualquer outro ambiente telemático. Ou seja, uma fraude em que o computador é usado como instrumento do crime, fora da internet, também seria alcançada pelo que se denominou “delitos informáticos” (Rossini, 2004, p. 110).

Ademais, a fim de buscar melhor compreensão, os cibercrimes foram classificados em crimes virtuais próprios/puros e crimes virtuais impróprios/impuros. O primeiro deles ocorre quando o sujeito ativo se utiliza do sistema informático do sujeito passivo para a pratica do crime, ou seja, o computador da vítima é o meio de execução e o próprio objeto do crime (Dambros, 2021). Logo, o bem jurídico protegido neste caso é a inviolabilidade de informações automatizadas (dados) (Viana, 2003 *apud* Carneiro, 2012).

> Nesse tipo de crime, não há apenas a intrusão de dados não autorizados, mas também toda interferência em dados informatizados, como a intrusão de dados armazenados no computador, para modificar, alterar, inserir dados errados, ou seja, uso direto do computador. Software ou hardware, e só pode ser implementado por um computador ou software ou hardware para computadores e seus dispositivos periféricos (Zaniolo, 2021, p. 50).

Assim, ao praticar um crime virtual próprio, o sujeito ativo tem a intenção de violar os dados digitais do sujeito passivo por meio do ingresso não autorizado no computador da vítima, obtendo, alterando ou inserindo dados. Como exemplo, destaca-se os *crackers*, pessoas que se utilizam de seu conhecimento técnico em informática para invadir sistemas privados com objetivo de obter vantagens ilícitas, consumando o crime no próprio ambiente virtual, sem gerar efeitos fora dele (Nascimento, 2016).

Já nos crimes virtuais impróprios, o computador será apenas o meio de execução, tendo em vista que o objeto do crime será diverso, ou seja, apesar de ser utilizado sistemas informáticos para a execução do delito, os bens jurídicos são diversos da informática (Rocha, 2017). Assim, para Nascimento (2016, p. 24), estes delitos ocorrem quando o "agente utiliza-se do computador e da internet como ferramenta para produzir um resultado que afeta outros bens tutelados pelo nosso ordenamento jurídico que não sejam relacionados aos meios virtuais". Como exemplo, a autora faz mesão ao artigo 241 do ECA, referente ao crime de divulgação de fotografias pornográficas de crianças e adolescentes.

Tais crimes tornam-se cada vez mais comuns, tendo em vista que hoje grande parte da população utiliza dispositivos informáticos para as mais diversas atividades, desde o trabalho, estudo e até mesmo para entretenimento. Segundo dados da consultoria alemã Roland Berger, em 2021, o Brasil ficou em quinto lugar no ranking dos países que mais sofreram com cibercrimes, totalizando 9,1 milhões de ocorrências (Globo, 2021). Sendo assim, a invasão em sistemas informáticos tornou-se uma oportunidade e um instrumento de lucro ilícito, que vem sendo cada vez mais utilizado (Rocha, 2017).

Ocorre que a prática destes delitos é preocupante, tento em vista que são extremamente complexos. O primeiro motivo, é pela facilidade da prática do crime, afinal, o agente pode atingir inúmeras vítimas, em qualquer lugar, além de poder agir em anonimato. Ademais, tais crimes são instáveis, ou seja, podem ser facilmente

apagados e alterados (Lorenzo; Scaravelli, 2021). Dessa forma, torna-se difícil encontrar provas de autoria e materialidade do delito, e até mesmo de definir o local do crime.

Em suma, pelo crime ser praticado em dispositivos informáticos, muitas de suas provas ficam armazenadas virtualmente, tornando cada vez mais comum a existência de provas digitais. Além disso, a prática de crimes cibernéticos exige que as autoridades realizem investigações em meios virtuais. Sendo assim, a coleta de provas e a investigação destes delitos tornam-se ainda mais complexas, já que há carência de leis, de estrutura e capacitação das autoridades.

2.5.2 Investigação criminais virtuais

As investigações criminais virtuais são realizadas quando a infração penal é praticada por meio do uso de sistemas informatizados, como por exemplo, a internet ou computador (Lessa; Vieria, 2017). Assim, as autoridades policiais precisam identificar qual foi o meio utilizado para a prática do delito (e-mail, contato telefônico, website, etc.) para saber em que local será realizada a investigação (Lessa; Vieria, 2017). Contudo, existem inúmeros impasses no processo investigatório, dificultando a obtenção de provas e responsabilização dos agentes.

Um dos primeiros problemas é a falta de leis específicas que regulamentem como devem ser realizadas tais investigações. Apesar de haver algumas normatizações, tais como a Lei 12.965/2014, conhecida como Marco Civil da Internet, esta já foi muito criticada pelos doutrinadores, ao ser considerada burocrática, por exigir ordem judicial para obtenção de dados, bem como por haver diversas lacunas (Lessa; Vieria, 2017). Além disso, a Lei 13.441/17 instituiu no ECA a infiltração de policiais em meio virtual para combate a crimes contra dignidade sexual de crianças e adolescentes, (Brasil, 2017), ocorre que não há lei que preveja a infiltração virtual em caso de pratica de outros crimes.

Outro impasse é a falta de estrutura dos órgãos de investigação, bem como a falta de conhecimento técnico das autoridades responsáveis, já que a mera criação ou alteração de leis não será suficiente para que haja a correta realização da investigação virtual e eficaz combate aos crimes cibernéticos. Assim, é necessário “um aparato técnico e específico nas investigações forenses por parte das polícias

quanto a estes delitos e uma ação conjunta entre os diversos entes que corporificam o Poder Judiciário e o Ministério Público” (Rocha, 2013, p. 8).

Além disso, outra preocupação é o tempo dispensado para a conclusão das investigações, já que a falta de regulamentação e, principalmente, a falta de estrutura e preparação policial acabam dificultando a obtenção de provas. Assim, muitos crimes virtuais prescrevem antes mesmo de ser finalizada a investigação (Lessa; Vieria, 2017).

Por fim, outra grande preocupação é como obter, preservar e utilizar corretamente as provas digitais encontradas durante estas investigações, já que não há regulamentação quanto a cadeia de custódia de uma prova digital. Afinal, a ignorância quanto as etapas a serem seguidas pode dar causa a quebra desta cadeia, prejudicando tanto as partes do processo, quanto a própria sociedade. Isso porque, desrespeitar o devido manejo de uma prova digital pode ocasionar impunidades por falta de provas, quando estas se tornam inutilizáveis ou, até mesmo, ocasionar injustiças, quando não verificada corretamente a sua validade e legalidade, dando causa a condenações de inocentes.

3 UMA NOVA ESPÉCIE DE PROVA: A PROVA PENAL DIGITAL

Após análise dos impactos da sociedade da informação no direito penal e processual penal, nota-se que uma das consequências desta evolução é a existência de provas digitais, as quais mostram-se cada vez mais presentes na persecução penal. Por possuírem natureza distinta das demais provas, mostra-se necessário estudá-las, a fim de conhecer o seu conceito, características e os meios de sua obtenção.

3.1 TEORIA GERAL DA PROVA PENAL

Para que seja possível compreender do que se trata a prova digital, bem como os meios de sua obtenção mediante as investigações virtuais, primeiramente, faz-se necessário uma breve análise da teoria geral da prova, a fim de compreender suas principais regras e finalidades no direito processual penal brasileiro.

3.1.1 A finalidade da prova e a importância da sua produção para a observância do devido processo legal

A fim de compreender a função e importância da prova para o processo penal, faz-se necessário analisar algumas premissas relativas à prova e ao processo. Primeiramente, verifica-se que com o passar do tempo, há uma maior humanização, não só na imposição de penas, mas também quanto a apuração dos delitos (Vaz, 2012), ainda que haja muito a melhorar neste aspecto.

Para Ferrajoli (2010), o processo penal serve tanto para reduzir os impactos que o crime causou na sociedade, como forma de diminuição da violência, mas, também serve para minimizar o arbítrio do Estado, já que apenas ele detém o *ius puniendi*. Ainda, em relação ao processo, importante destacar que existem dois modelos, o inquisitório e o acusatório.

O sistema inquisitório é caracterizado pela concentração do poder nas mãos do juiz inquisidor, o qual reúne tripla função, a de acusar, defender e julgar, comprometendo a sua imparcialidade e a garantia do contraditório. Além disso, este sistema admite ampla atividade probatória, acreditando ser possível a descoberta da verdade real/absoluta, já que esta é buscada a qualquer custo. Logo, tal sistema revela-se incompatível com os direitos e garantias fundamentais (Lima, 2020).

Já o acusatório, trata-se do sistema adotado pelo Brasil, tanto pela Constituição Federal, ao prever diversas garantias e a função privativa do Ministério Público nas ações penais públicas (Lima, 2020), quanto para a maioria da doutrina e para jurisprudência do STF[7] (Dezem, 2016). Também, destaca-se o artigo 3º-A do Código de Processo Penal, que apesar de suspenso, prevê expressamente a estrutura acusatória (Brasil, 2019). Porém, como certeiramente aponta Lopes Junior (2020), apesar de constitucionalmente acusatório, para efetivação deste sistema "é imprescindível afastar a vigência de vários artigos do CPP e mudar radicalmente as práticas judiciárias" (Lopes Júnior, 2020, p. 71). Logo, tendo em vista ser o sistema adotado pelo ordenamento jurídico brasileiro, torna-se importante analisar suas características para entender a funcionalidade e importância da prova.

Esse sistema caracteriza-se pela divisão de funções, ou seja, haverá um órgão de defesa, um de acusação e outro de julgamento (Dezem, 2016). Desta forma, graças a separação da função de acusar e julgar, tal sistema é caracterizado pela inércia e imparcialidade do juiz (Lima, 2020). Logo, o julgador não poderá iniciar o processo de oficio, nem mesmo ser o gestor da prova, cabendo a iniciativa apenas à acusação, e a produção da prova apenas às partes, salvo exceções, como preceitua o artigo 156 do Código de Processo Penal[8] (Brasil, 1941).

Diante disso, quanto à matéria probatória, o juiz só será responsável por valorar aquelas já produzidas pelas partes, a fim de chegar a uma decisão final (Neto; Lopes, 2022). Esta valoração será feita por meio do livre convencimento motivado, ou seja, o juiz não está subordinado a nenhuma regra específica, podendo valorá-las livremente (Dezem, 2016). No entanto, este convencimento encontra limitações, não podendo o juiz decidir de acordo com sua íntima convicção, devendo fundamentá-la dentro das regras processuais penais e constitucionais (Neto; Lopes, 2022). Neste sentido, aponta Lopes Júnior (2020, p. 610):

> Em definitivo, o livre convencimento é, na verdade, muito mais limitado do que livre. E assim deve sê-lo, pois se trata de poder e, no jogo democrático do processo, todo poder tende a ser abusivo. Por isso, necessita de controle. Não se pode pactuar com o decisionismo de um juiz que julgue 'conforme a

[7] STF, ADIn 5104 MC-DF, j. 21.05.2014, rel Min. Roberto Barroso.

[8] Art. 156. A prova da alegação incumbirá a quem a fizer, sendo, porém, facultado ao juiz de ofício: I – ordenar, mesmo antes de iniciada a ação penal, a produção antecipada de provas consideradas urgentes e relevantes, observando a necessidade, adequação e proporcionalidade da medida; II – determinar, no curso da instrução, ou antes de proferir sentença, a realização de diligências para dirimir dúvida sobre ponto relevante (Brasil, 1941, não paginado).

> sua consciência', dizendo 'qualquer coisa sobre qualquer coisa'. Não se nega a subjetividade, por elementar, mas o juiz deve julgar conforme a prova e o sistema jurídico penal e processual penal, demarcando o espaço decisório pela conformidade constitucional.

Por fim, diferente do inquisitório que busca a verdade real ou absoluta, o sistema acusatório adota o princípio da busca da verdade (Lima, 2020), ou também chamada de verdade formal ou processual (Lopes Júnior, 2020). Este princípio estabelece limites à produção probatória, ao entender que não se pode buscar a verdade a qualquer custo, exigindo-se respeito às garantias constitucionais e processuais (Lopes Júnior, 2020). Além disso, para Ferrajoli (2010), a verdade fática é o que aconteceu no mundo dos fatos, já a verdade formal trata-se de uma aproximação daquela, ou seja, é o que se sabe, o que está reunido no processo, desde que respeitadas as regras e garantias.

Diante disso, nota-se que a prova tem dupla função, a busca da verdade aproximada, bem como o convencimento do órgão julgador. Assim, percebe-se que a prova está intimamente ligada às finalidades do processo penal, já que é graças a ela que se possibilitará a responsabilização do agente e a manutenção da ordem, mas também servirá de limite ao poder punitivo do Estado, evitando autoritarismos e erros judiciais. Logo, a prova é ferramenta importante para o cumprimento do devido processo legal.

3.1.2 Conceitos e o procedimento da prova penal

Após breve análise da função e importância da prova para o processo penal, será possível compreender o seu conceito. Porém, a palavra prova possui caráter polissêmico, não havendo uma conceituação única pela doutrina (Dezem, 2016). Diante disso, cabe analisar algumas das conceituações doutrinárias referente ao tema.

Para Lopes Júnior, prova trata-se de um "ritual de recognição", o qual possibilita o exercício da "atividade recongnitiva" pelo juiz (p. 556-557, 2020). Ou seja, é a reconstrução aproximada de um fato determinado passado, oportunizando ao juiz o conhecimento daquilo que ignora.

Já para Lima (2020, p. 657) a palavra prova significa "verificação, inspeção, exame, aprovação ou confirmação". Além disso, o autor destaca que a prova possui três acepções, sendo considerada como atividade, meio e resultado, ou seja, a prova

trata-se de atos praticados pelas partes durante o processo em busca da demonstração da veracidade ou não de determinado fato (atividade probatória), por meio de instrumentos idôneos (meio), em busca da convicção do órgão julgador (resultado) (Lima, 2020). Ainda, de acordo com Giacomolli:

> A palavra prova, no processo penal, passou a demonstrar tudo o que ela pertine, ou seja, os meios empregados na demonstração dos fatos ou do thema probandum, a atividade utilizada pelas partes para levar ao processo os meios de prova, bem como o próprio resultado do procedimento probatório, ou seja, convencimento exteriorizado pelo julgador (Giacomolli, 2015, p. 172).

Em suma, apesar destes e outros conceitos, é possível tecer um entendimento básico referente a prova. Logo, pode se dizer que prova são todos os elementos colhidos durante o processo, em busca da demonstração da veracidade ou não do fato imputado ao agente, com o fim de convencer o órgão julgador no momento da decisão. Além disso, cabe destacar que “o vocábulo prova é utilizado para designar diferentes aspectos do fenômeno probatório: fonte de prova, meio de prova, elemento de prova, resultado probatório e procedimento probatório” (Vaz, 2012, p. 45).

As fontes de provas são todas as pessoas e/ou coisas, por meio das quais as provas podem ser obtidas, sendo ainda classificadas em fontes reais e fontes pessoais (Lima, 2020). As fontes pessoais referem-se as testemunhas, peritos e partes do processo, já a fonte real refere-se a todas as demais (Vaz, 2012). Ainda, cabe destacar que a fonte é considerada extraprocessual, tendo em vista que “decorre do fato em si, independentemente da existência de um processo” (Badaró, 2003, p. 164-166).

Por sua vez, meios de prova são os instrumentos utilizados para introduzir as provas no processo, tratando-se de uma atividade endoprocessual, ou seja, só se desenvolve após iniciado o processo, perante o juiz (Lima, 2020). Logo, como um exemplo, a pessoa que presencia os fatos é uma fonte de prova (testemunha), já a sua declaração em juízo (testemunho) é o meio de prova, tendo em vista que é através dele que a prova será introduzida no processo.

Ademais, quanto ao elemento de prova, este refere-se a todos os dados probatórios que foram inseridos no processo e que servirão para confirmar ou negar um fato de interesse da causa (Vaz, 2012). Já o resultado da prova, é a conclusão da análise de todos estes elementos colhidos no processo, que serão capazes de determinar se os fatos foram provados ou não (Vaz, 2012).

Por fim, quanto ao procedimento probatório, Aranha (2008, p. 35) o define como sendo “a marcha dos atos processuais relativos à prova, na forma prevista pela lei e de maneira coordenada e concatenada”. Ainda, Avena (2022) aponta quatro fases da produção probatório.

A primeira delas, nominada de preposição, é o momento em que as partes requerem a produção das provas ao julgador, podendo ocorrer ordinariamente, quando o pedido ocorre na denúncia ou queixa e na resposta à acusação, ou então de forma extraordinária, isto é, após iniciada ou encerrada a instrução. Após a preposição, sobrevêm a fase da admissão, que se refere ao momento em que o juiz decidirá sobre o deferimento ou não das provas requeridas (Avena, 2022).

Depois, passa-se para a fase da produção das provas que foram deferidas pelo magistrado. Por fim, a última fase é a valoração, quando o juiz prolatará a sentença, momento em que analisará cada uma das provas produzidas, dando a elas o valor que julgar pertinente (Avena, 2022).

3.1.3 Princípios que regem a prova penal

Após a análise dos preceitos básicos atinentes a prova, cabe por fim compreender quais são os princípios que devem ser observados durante todo o procedimento probatório. Primeiramente, destaca-se o princípio da presunção da inocência, previsto no artigo 5º, inciso LVII, da Constituição Federal, bem como no artigo 8ª da Declaração Universal dos Direitos Humanos, o qual, para Lopes Júnior “trata-se do princípio reitor do processo penal” (2020, 589), possuindo três dimensões: norma de tratamento, norma probatória e de julgamento (Lopes Júnior, 2020).

Quanto à norma de tratamento, o autor ainda divide em interna e externa. A primeira delas exige que o Juiz trate o acusado como inocente até o trânsito em julgado da condenação, já o tratamento externo refere-se ao restante da sociedade, vedando publicidades abusivas e estigmatizações. Por outro lado, a norma probatória entende que o ônus de provar é da acusação, além de que só podem ser admitidas provas lícitas. Por fim, a norma de julgamento impõe que o Juiz decida com base nas provas produzidas, e, caso estas não sejam suficientes, deve ser aplicado o *in dubio pro reo* (Lopes Júnior, 2020).

Outro importante princípio é o da oralidade, o qual em seu sentido estrito, significa a utilização da palavra verbal, motivo pelo qual exige-se a palavra falada em

juízo, devendo as testemunhas se manifestar oralmente perante o juiz em audiência (Pereira, 2010). Com isso, possibilita-se que o juiz avalie a sinceridade do depoimento, o que não seria possível se a prova fosse colhida de forma escrita, uma vez que esta impossibilita a averiguação da veracidade dos fatos, ferindo o princípio do contraditório (Nucci, 2015).

Já em sentido amplo, o princípio é dividido em outros quatro subprincípios. O da imediação significa que o juiz deve colher as provas em contato direito com as partes, porém, há uma mitigação prevista no artigo 189 do CPP, o qual autoriza o interrogatório por videoconferência em alguns casos excepcionais (Avena, 2022). Já o segundo é o princípio da concentração dos atos processuais, o qual entende que se deve tentar colher as provas em uma única audiência, em busca da celeridade. O terceiro, trata-se da irrecorribilidade das decisões interlocutórias, com o objetivo de evitar a interrupção do processo (Lima, 2020). Por fim, o quarto e último subprincípio é o da identidade física do juiz, isto é, o juiz que preside a instrução deve proferir a sentença (Lima, 2020).

> Louvável a introdução desse princípio no processo penal, já que, antes da reforma processual de 2008, era extremamente comum que um juiz interrogasse o acusado, outro ouvisse as testemunhas de acusação, outro as de defesa, com um quarto magistrado proferindo a sentença. Esse distanciamento entre a prova e o magistrado prejudicava a formação de um quadro probatório coeso e harmônico, prejudicando um dos escopos do processo penal, que é a busca da verdade (Lima, 2020, p. 711).

No entanto, a jurisprudência entende haver exceções a esse princípio, devendo ser aplicado o artigo 132 do Código de Processo Civil. Sendo assim, outro juiz poderá julgar, caso o da instrução estiver convocado, licenciado, afastado, promovido ou aposentado (Dezem, 2016).

Também, importante destacar o princípio da autorresponsabilidade das partes, o qual entende que as partes devem assumir as consequências quanto a prova de suas alegações. Assim, por exemplo, caso a acusação não consiga provar os fatos constantes na denúncia/queixa, a consequência será a absolvição, ou então, caso a defesa arrole uma testemunha, e esta incrimine o réu, o juiz poderá utilizá-la (Avena, 2022).

Ademais, outro princípio a ser observado é o da comunhão da prova, isto é, após ser produzida, esta não pertencerá a nenhuma parte, nem mesmo ao juiz. Sendo

assim, este princípio permite que qualquer parte utilize as provas constantes no processo, ainda que seja a outra quem a tenha produzido (Lima, 2020).

Além disso, não se pode deixar de mencionar o princípio da não autoincriminação, também conhecido como *nemo tenetur se detegere,* o qual estabelece que o acusado não é obrigado a produzir provas contra si. Daí advêm alguns direitos ao acusado, tais como permanecer em silêncio, podendo se recusar a responder perguntas durante seu interrogatório, sem que isso lhe prejudique (Avena, 2022).

Por fim, destaca-se também o princípio da liberdade probatória, o qual proporciona ao processo penal brasileiro ampla liberdade, seja quanto ao momento da prova, quanto ao seu tema e também quanto aos meios utilizados. Sendo assim, a prova pode ser produzida a qualquer momento, apesar de haver algumas exceções, tais como a prova testemunhal e os documentos e objetos a serem juntados nos processos de competência do júri (Avena, 2022).

Ainda, é permitido utilizar qualquer meio de prova, desde que o objeto não verse sobre o estado da pessoa, nem viole a lei, os princípios e a moral social. Já quanto ao tema, admite-se a produção da prova sobre qualquer fato que seja considerado importante para o processo, porém, caso sejam irrelevantes, impertinentes ou protelatórias, o juiz estará autorizado a indeferi-las (Lima, 2020).

Em suma, a observância de todos estes princípios/garantias é imprescindível para concretização do devido processo legal e a busca pela decisão mais justa. Sendo assim, após entendimento do conceito, finalidade e importância da prova para o processo penal, bem como algumas regras e princípios básicos que devem ser observados em qualquer espécie de prova, será possível compreender do que se trata a prova penal digital.

3.2 A PROVA PENAL DIGITAL

Feita uma breve análise do contexto atual da sociedade, percebe-se que a tecnologia da informação está gerando impactos e constantes mudanças em diversos aspectos do direito criminal, sendo a prova digital um exemplo disso. Assim, tal fato torna-se preocupante, já que, como analisando anteriormente, a prova possui papel fundamental no processo penal, logo, deve ser utilizada adequadamente, a fim de garantir um devido processo legal. No entanto, como explica Badaró (2021), há vários

impasses relacionados a esta nova espécie de prova, não só pela falta de legislação específica, mas também pela rápida mutação da tecnologia informática.

Sendo assim, diante da complexidade de tal temática, faz-se necessário um estudo relativo ao conceito, classificação, características e validade da prova penal digital, a fim de compreendê-la.

3.2.1 Conceito, classificação e natureza jurídica

Para Machado (2022), as provas digitais distinguem-se das demais espécies tradicionais, pois são extraídas de dados informáticos. Além disso, Casey (2004, p. 12), conceitua a prova digital como sendo “qualquer dado armazenado ou transmitido usando um computador que confirma ou rejeita uma teoria a respeito de como ocorreu um fato ofensivo ou que identifica elementos essenciais da ofensa como intenção ou álibi”. Já para Vaz, trata-se de “dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias” (2012, p. 63).

Ademais, apesar da legislação processual penal vigente não prever uma conceituação, o Projeto do Novo Código de Processo Penal conceitua tal prova como sento “toda informação armazenada ou transmitida em meio eletrônico hábil ao esclarecimento de determinado fato” (Sarney, 2010, p. 480). Também, destaca-se a conceituação trazida por Rodrigues, que define a “prova electrónico-digital” como sendo (2016, p. 39):

> Qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digital de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binaria ou digital.

Por outro prisma, Mendes (2019) entende ser complexa a conceituação da prova digital, já que há confusão entre a conceituação desta e a prova eletrônica. Para o autor, a prova eletrônica é uma das espécies de prova, tratando-se de todos aqueles equipamentos eletrônicos, ou seja, suportes físicos que armazenam dados digitais. Já a prova digital trata-se de uma subespécie, tendo em vista que se refere aos dados produzidas/armazenadas em meios informáticos.

Diante disso, a prova eletrônico-digital nada mais é do que informações e dados que são produzidos e/ou armazenados digitalmente, contidos em dispositivos físicos, como computadores, celulares, *pen drives* e câmeras*,* os quais podem produzir e armazenar vídeos, fotos, áudios, mensagens, fotografias, e também aquelas informações contidas em meios informáticos, tais como o ciberespaço, a nuvem, e-mails, comércios on-line, redes sociais e tantos outros, os quais serão utilizados para confirmar ou rejeitar determinado fato no processo.

Além disso, quanto à sua classificação, Vaz (2012) sustenta que a prova digital é fonte de prova, ou seja, trata-se do meio pelo qual a prova é obtida, “local de onde podem ser extraídas as informações de interesse da persecução penal” (Vaz, 2012, p. 63). Neste mesmo sentido, a autora entende que prova digital “não compreende os meios de prova que se utilizam de sistema informático para auxiliar na interpretação e análise de dados. É o caso de animações ou simulações elaboradas no computador, assim como reconstituições de fatos em programas informáticos” (Vaz, 2012, p. 63).

Também não compreendem “as informações que possam ser obtidas de entidades públicas ou de terceiros, por meio de requisição, apenas porque sejam registradas em meios digitais” (Vaz, 2012, p. 64), como por exemplo, os dados bancários de um investigado. Logo, prova digital não se trata de mera obtenção de informação em meio digital, mais sim, por exemplo, de dados armazenados no sistema informático de um banco, que sejam capazes de trazer informações úteis na busca da verdade de um crime praticado pelo investigado (Vaz, 2012).

Ainda quanto à sua classificação, trata-se de uma prova atípica, já que não está prevista de forma explicita na legislação penal brasileira (Lemos; Cavancante; Mota, 2021). Apesar disso, a prova digital é admitida no direito penal brasileiro, já que o legislador não é capaz de prever e regular todas as espécies de provas existentes, mas desde que sua utilização não viole o ordenamento jurídico (Fernandes, 2019). Em suma, a prova digital, apesar de atípica, tende a ser amplamente utilizada na persecução penal, já que é cada vez mais comum a produção e armazenamento de informações em meios digitais.

Por fim, quanto à natureza jurídica, Vaz (2012) aponta como sendo uma prova documental, apesar de possuir algumas características distinta daquela prevista em lei. O Código de Processo Penal conceitua a prova documental como sendo “quaisquer escritos, instrumentos ou papéis, públicos ou particulares” (Brasil, 1941). Diante desta conceituação, Vaz (2012) entende que a prova digital pode ser

considerada documental, já que engloba escritas, imagens, fotografias, entre outras formas de representação de um fato, as quais podem ser materiais ou imateriais, isto é, armazenadas em meios eletrônicos.

3.2.2 Características

A prova digital é uma espécie singular, ou seja, única e distinta das demais. Por este motivo, carrega características próprias, das quais, Vaz (2012) enumera quatro delas: a imaterialidade, a volatilidade, a suscetibilidade de clonagem e a necessidade de intermediação.

Primeiramente, quanto à imaterialidade, trata-se de uma prova incorpórea, não sendo necessário um suporte físico, o que possibilita sua transferência por redes de comunicação ligadas a dispositivos eletrônicos e digitais, ou seja, sem a necessidade de movimentação física, bem como possibilita grande armazenamento de informações (Vaz, 2012).

Quanto à volatilidade, refere-se à possibilidade de alteração que esta prova possui, o que pode causar mudanças constantes ou perdas de informações. Por este motivo é que Vaz entende ser necessária uma técnica específica para manejo desta prova, a fim de preservá-la. Ainda, a prova digital é suscetível de clonagem, haja vista que é possível transferir integralmente um dado ou informação de um dispositivo informático para outro, admitindo assim, inúmeras cópias (Vaz, 2012).

Por fim, a última característica apontada pela autora é a necessidade de intermediação, ou seja, apesar da prova digital não necessitar de um suporte físico, exige-se a utilização de equipamentos para processar a informação e transmiti-la ao ser humano de forma compreensível (Vaz, 2012). Em virtude destas características, Badaró (2021, p. 2) entende que:

> há necessidade de uma maior preocupação com a possibilidade de falsificação ou destruição. Há, na prova digital, uma “congênita mutabilidade”. Em suma, trata-se de fonte de prova que pode ser facilmente contaminada, sendo sua gestão muito delicada, por apresentar um alto grau de vulnerabilidade a erros.

Diante disso, nota-se que a prova digital exige maior cuidado, uma vez que pode ser facilmente manipulada ou extraviada. Por este motivo, Souza (2021) defende

que a prova digital pertence ao gênero das provas científicas, pois exige-se a utilização de um método específico e de um responsável com qualificação técnica para coletar, tratar e armazenar corretamente a prova digital.

3.3 OS MEIOS DE OBTENÇÃO E PRODUÇÃO DA PROVA PENAL DIGITAL: UMA NOVA FORMA DE INVESTIGAÇÃO

Para melhor compreensão da prova digital, importante elencar quais são as formas de obtenção e produção desta espécie de prova. Porém, tal tarefa é difícil, afinal, não há lei no Brasil que defina quais são estes meios.

Diante desta lacuna, importante destacar a obra de Vaz (2012), a qual elenca quais seriam. Para a autora, a prova digital fica armazenada em um dispositivo eletrônico ou trafega na rede por meio da internet, logo, estas são as fontes da prova digital, objetos por meio dos quais elas são obtidas. Já os meios de obtenção, referem-se à busca e apreensão de suportes físicos e apreensão remota de dados, ou seja, tratam-se de instrumentos utilizados para introduzir estas provas no processo penal. Por fim, quanto à produção da prova penal digital, esta refere-se ao modo como pode ser apresentada em juízo, podendo ser de forma documental ou pericial (Vaz, 2012).

Além disso, também importante mencionar o Projeto de Lei n.º 4.939/20, o qual tem por objetivo definir as regras de obtenção e admissibilidade da prova digital:

> Art. 9º Constituem meios de obtenção da prova digital, na forma da Lei:
> I – a busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo.
> II – a coleta remota, oculta ou não, de dados em repouso acessados à distância.
> III – a interceptação telemática de dados em transmissão.
> IV – a coleta por acesso forçado de sistema informático ou de redes de dados.
> V – o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial. (Leal, 2020, p. 4-5).

Sendo assim, será feita uma análise quanto a estes meios de prova elencados pela autora, em conjunto com o Projeto de Lei n.º 4.939/20 e as leis existentes sobre o tema.

3.3.1 Busca e apreensão de dispositivos eletrônicos e sistemas informáticos

Primeiramente, quanto ao seu conceito, importante destacar que busca e apreensão são duas coisas distintas. A busca trata-se da realização de diligências com a finalidade de localizar determinado objeto ou pessoa. Já a apreensão é uma medida de constrição, ficando o objeto ou pessoa sob custódia (Lima, 2020). Por este motivo é que nem sempre a busca dará causa a uma apreensão, e a apreensão nem sempre decorrerá da busca (Lopes Júnior, 2020).

Apesar de prevista no Código de Processo Penal dentre as espécies de prova, trata-se na verdade de meio de obtenção, com objetivo de acautelar e assegurar a prova, sendo subdividida em duas espécies, a busca domiciliar e a busca pessoal (Lima, 2020).

Quanto a busca domiciliar, trata-se da busca realizada na casa[9] do indivíduo, com objetivo de apreender pessoas e/ou coisas elencadas no artigo 240, §1º, do Código de Processo Penal[10]. No entanto, por ser a casa asilo inviolável, exige-se que a busca e apreensão ocorra durante o dia[11], por meio de mandado judicial devidamente fundamentado, não se exigindo estes requisitos se houver flagrante delito, consentimento válido, desastre ou para prestação de socorro (Lima, 2020).

De outro modo, a busca pessoal ocorre quando há fundada suspeita de que a pessoa oculte consigo: coisas achadas ou obtidas por meio criminoso; instrumentos de falsificação ou objetos falsificados; armas e munições instrumento do crime; objetos necessários para provar a infração ou servir de defesa do réu; ou para colher qualquer outro elemento de convicção (Brasil, 1941).

---

[9] A casa é “a) qualquer compartimento habitado; b) aposento ocupado de habilitação coletiva, ainda que se destine à permanência por poucas horas; c) compartimento não aberto ao público, onde alguém exerce profissão ou atividade” (Lima, 2020, p. 799).

[10] Art. 240. A busca será domiciliar ou pessoal.
§ 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para:
a) prender criminosos;
b) apreender coisas achadas ou obtidas por meios criminosos;
c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos;
d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso;
e) descobrir objetos necessários à prova de infração ou à defesa do réu;
f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;
g) apreender pessoas vítimas de crimes;
h) colher qualquer elemento de convicção (Brasil, 1941, não paginado)

[11] O dia corresponde ao período das 6 horas às 18 horas (Lima, 2020).

Porém, como pode-se perceber da análise dos artigos 240 a 250 do Código de Processo Penal, não há previsão quanto a busca e apreensão de dispositivos eletrônicos, tais como computadores e celulares dos investigados (Brasil, 1941). Diante disso, apesar desta lacuna Vaz (2012), entende que a busca e apreensão pode também ser utilizada para: apreender arquivos digitais obtidos por meio criminoso; apreender arquivos digitais falsificados e apreender dispositivos eletrônicos que foram utilizados para pratica da infração penal.

Para tanto, Vaz (2012) aponta algumas formalidades que devem ser seguidas, antes, durante e após realizada a busca e apreensão. Antes de iniciar a busca, faz-se necessário autorização judicial, devendo o mandado ser dirigido aos locais em que se encontram os dispositivos eletrônicos que possam conter informações de interesse para a investigação ou processo. Também, destaca a autora, que a busca e apreensão deve recair somente sobre os dispositivos eletrônicos do investigado, e não sobre todos que estejam localizados na casa (Vaz, 2012).

Durante a busca e apreensão, por se tratar de prova volátil, Vaz (2012) defende ser necessária a presença de perito ou técnico na área de informática, com o fim de prevenir a autenticidade da prova, evitando sua perca ou alteração. Ainda, encontrados os dispositivos eletrônicos, estes só podem ser apreendidos ou copiados pelo expert, não podendo haver intervenção no seu conteúdo (Vaz, 2012).

Por fim, após realizada a busca, bem como a apreensão ou cópia dos dispositivos eletrônicos, deve ser produzido auto detalhado da diligência. Caso tenha havido a apreensão, os objetos devem ser lacrados e o auto deve conter quais dispositivos eletrônicos foram apreendidos, indicando a descrição, a marca, o modelo e o estado em que se encontra no momento da diligência. Por outro lado, caso tenha havido cópia da memória do dispositivo, deve constar qual o procedimento adotado, a descrição dos dispositivos eletrônicos que detinham as informações que foram copiadas, bem como o suporte que recebeu a cópia (Vaz, 2012).

Diante destes apontamentos da autora, verifica-se que há duas grandes preocupações envolvendo este tipo de busca e apreensão, a primeira delas é a proteção ao direito de privacidade e intimidade, exigindo-se mandado judicial para verificar os dispositivos eletrônicos do investigado, bem como vedando-se a busca e apreensão de dispositivos que não tenham relação com a investigação. A segunda preocupação é a proteção da prova digital, exigindo-se procedimento para coleta, a

ser realizado por profissionais da área, bem como o registro da diligência, a fim de evitar a perda ou modificação da prova.

Além dos apontamentos de Vaz, importante mencionar o Projeto de Lei n.º 4.939/20, o qual prevê algumas regras a serem adotadas atinentes a busca e apreensão da prova digital. Primeiramente, destaca-se que o Projeto não traz procedimento específico e detalhado do passo a passo, mas sim algumas regras gerais aplicáveis a qualquer meio de obtenção de prova digital, tais como a exigência de mandado judicial; a presença de perito oficial ou técnico de informática; a elaboração de auto circunstanciado e registro da custódia (Leal, 2020). Assim, o Projeto contém apenas dois artigos específicos em relação a busca e apreensão, os quais preveem a exigência de espelhamento da prova digital:

> Art. 21 Salvo expressa determinação judicial em contrário ou impossibilidade de cumprimento da medida desta forma, a apreensão da prova digital ocorrerá por espelhamento, não se fazendo a apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica (Brasil, 2020, p. 08).
>
> Art. 22 Em caso de impossibilidade de apreensão por espelhamento, será garantida aos titulares ou agentes de tratamento atingidos pela apreensão dos dispositivos eletrônicos, sistemas informáticos ou outros meios de armazenamento de informação eletrônica cópia dos dados coletados. A apreensão não poderá superar 60 (sessenta) dias, salvo por motivo relevante (Brasil, 2020, p. 09).

Sendo assim, para o Projeto, deve haver o espelhamento do dispositivo eletrônico, sendo permitida a apreensão somente quando aquele mostrar-se impossível. Ocorre que o referido Projeto diverge com os entendimentos recentes dos Tribunais Superiores, como exemplo, destaca-se a decisão do Superior Tribunal de Justiça que entendeu não ser cabível a obtenção de prova por meio do espelhamento do Whatsapp, utilizando-se do WhatsApp Web (HC 99.735/SC).

> No espelhamento via WhatsApp Web o investigador de polícia tem a concreta possibilidade de atuar como participante tanto das conversas que vêm a ser realizadas quanto das conversas que já estão registradas no aparelho celular, haja vista ter o poder, conferido pela própria plataforma online, de interagir nos diálogos mediante envio de novas mensagens a qualquer contato presente no celular e exclusão, com total liberdade, e sem deixar vestígios, de qualquer mensagem passada, presente ou, se for o caso, futura. 8. O fato de eventual exclusão de mensagens enviadas (na modalidade "Apagar para mim") ou recebidas (em qualquer caso) não deixar absolutamente nenhum vestígio nem para o usuário nem para o destinatário, e o fato de tais mensagens excluídas, em razão da criptografia end-to-end, não ficarem armazenadas em nenhum servidor, constituem fundamentos suficientes para

> a conclusão de que a admissão de tal meio de obtenção de prova implicaria indevida presunção absoluta da legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica (Brasil, 2018, p. 02).

Assim, tal ferramenta possibilitaria que o investigador visualizasse todas as conversas passadas, presentes e futuras, inclusive podendo participar do diálogo, como se fosse o próprio investigado, sendo que qualquer alteração ou exclusão de mensagem não ficaria registrada, tendo em vista a existência de criptografia de ponta a ponta.

Diante de tantas peculiaridades envolvendo a busca e apreensão da prova digital, dando causa a entendimentos diversos, é notória a necessidade de uma lei que regulamente o procedimento a ser adotado, antes, durante e depois da busca e apreensão, a fim de possibilitar que as informações digitais colhidas possam ser usadas como prova no processo penal, bem como evitar a violação de garantias do investigado.

3.3.2 A apreensão remota de dados: interceptação e a infiltração em sistemas

Como visto acima, a forma mais utilizada para obtenção de prova digital em suportes físicos é a busca e apreensão, apesar de haver discussões quanto a possibilidade da adoção do espelhamento destes aparelhos eletrônicos. Ocorre que os dados não estão localizados só em suportes físicos, mas também em meios remotos, pelas redes virtuais. Assim, nestes casos não há necessidade de violação do domicílio, nem da restrição de direitos da propriedade, existindo outros meios de obtenção da prova, quais sejam, a interceptação telemática e telefônica; a infiltração em sistemas informáticos, por meio da implantação de softwares ou de programas maliciosos (Vaz, 2012).

A interceptação é o único meio de obtenção de prova digital que se encontra regulamentado, previsto na Lei 9.296/96. No seu artigo 1º, o dispositivo legal prevê a regulamentação da interceptação telefônica, já o parágrafo único estabelece que as mesmas regras serão aplicadas à interceptação telemática (Brasil, 1996). Para que seja possível compreendê-las, Lima (2020), ressalta que a palavra interceptar, neste caso, não significa interromper, deter ou impedir, mas sim, a forma pela qual será captada uma comunicação telefônica ou telemática alheia. Ou seja, trata-se da

“participação de um terceiro, que passa a ter ciência do conteúdo de uma comunicação alheia” (Lima, 2020, p. 812).

Ainda, Kist (2019) entende que a interceptação é destinada a busca de dados que estão sendo produzidos instantaneamente, e não de dados que se encontram armazenados em dispositivos eletrônicos. Ademais, Vaz (2012) compreende como sendo a “captação de dados em trânsito, que estejam sendo transmitidos por uma rede de dispositivos eletrônicos”[12].

Também, importante ressaltar que a interceptação não se limita a conversas por telefone (interceptação telefônica), abrangendo também o recebimento ou transmissão de imagens, símbolos, escritos, vídeos, sons, ou informações de qualquer natureza (interceptação telemática) (Lima, 2020).

Esta espécie de meio de prova digital, é dividida em outras três subespécies. A primeira é a interceptação em sentido estrito, a qual ocorre quando o terceiro intercepta a conversa sem conhecimento dos interlocutores. Já a segunda forma é a escuta telefônica, quando um dos interlocutores tem ciência de que a conversa está sendo interceptada. Por fim, a terceira refere-se à gravação telefônica, quando não há existência de um terceiro, sendo que um dos próprios interlocutores grava a conversa, sem os demais terem conhecimento, isto é, trata-se de uma autogravação (Fernandes, 2019).

Dentre estas subespécies, apenas a interceptação em sentido estrito é regulamentada em Lei, sendo que as demais foram aceitas pela jurisprudência (Vaz, 2012). Porém, apesar da interceptação ser admitida, é importante lembrar que o artigo 5º, inciso XII da Constituição Federal, prevê a inviolabilidade do sigilo das comunicações telefônicas (Brasil, 1998).

Logo, só é possível violar este sigilo seguindo uma série de requisitos, previstos nos artigos 1º e 2º da Lei 9.296/96, quais sejam: necessidade de ordem judicial fundamentada; utilização apenas para obtenção de provas em investigações criminais e instruções processuais penais; indício razoável de autoria ou participação; a prova não puder ser obtida por outro meio e, por fim, a pena cominada deve ser de

[12] Exemplificando a diferença entre a busca e apreensão e a apreensão remota de dados, caso alguma mensagem, esteja armazenada no Whatsapp, é cabível a busca e apreensão do celular, vez que se encontra em um suporte físico. Por outro lado, caso haja mensagens que estejam sendo enviadas e recebidas em tempo real, para sua obtenção será possível a apreensão remota de dados, seja por meio de um terceiro, pelo próprio interlocutor ou por um software instalado.

reclusão (Brasil, 1996). Dentre estas formalidades, há uma exceção, qual seja, a não exigência de ordem judicial quando se tratar de interceptação na modalidade de gravação eletrônica:

> Ao tratar da interceptação telefônica, admitindo-a, por ordem judicial, nas hipóteses e na forma que fosse estabelecida em lei, para fins de investigação criminal e instrução processual penal (art. 5º, XII, parte final), a Constituição Federal refere-se à interceptação feita por terceiro, sem conhecimento dos dois interlocutores ou com conhecimento de um deles. Não fica incluída a gravação de conversa por terceiro ou por um dos interlocutores, à qual se aplica a regra genérica de proteção à intimidade e à vida privada do art. 5º, X, da Carta Magna (Lima, 2020, p. 813).

Diante disso, considerando que a Constituição Federal não prevê a inviolabilidade do sigilo nesta hipótese, é possível que a gravação telefônica, isto é, a gravação da conversa por um dos interlocutores, possa ocorrer sem autorização judicial. Para tanto, é necessário que esta gravação esteja aparada por uma justa causa, ou seja, quando a gravação é “utilizada para comprovar a inocência do acusado ou quando houver investida criminosa de um interlocutor contra o outro (Lima, 2020, p.14). Ademais, apesar de haver divergência quanto a (i)licitude da gravação telefônica, tanto o STF quanto o STJ possuem precedentes que apontam para a licitude, conforme verifica-se na decisão do HC Nº 63.562 - ES (2015/0215095-4) (Brasil, 2015).

Quanto ao prazo, o artigo 5º da referida Lei, prevê que a diligência não pode exceder 15 dias, sendo cabível a renovação por igual período. Ocorre que o artigo não delimita a quantidade de renovações, por este motivo, há entendimento no sentido de evitar o prolongamento do prazo por grande período, vez que a norma restringe direitos fundamentais (Vaz, 2012). No entanto, em decisão recente, o STF autorizou a renovação sucessiva da interceptação telefônica, como se verifica da decisão dos Embargos de Declaração no Recurso Extraordinário n.º 625.263, do Paraná, em 2022 (Brasil, 2022).

No entanto, como pode-se perceber, a Lei 9.296/96 prevê apenas quais os requisitos devem ser preenchidos para admissibilidade da utilização da interceptação telefônica ou telemática, bem como o prazo para realização da diligência. No entanto, o referido dispositivo legal não dispõe quanto ao procedimento que deve ser seguido antes, durante e após a obtenção da prova. Sendo assim, conclui-se que tanto a busca

e apreensão de provas digitais, quanto a interceptação, carecem de normas referentes a cadeia de custódia, o que põem em risco a autenticidade e validade da prova.

3.3.3 Os meios de produção da prova digital: pericial e documental

Após obtidas as provas digitais, é preciso saber qual o meio de produção de prova será utilizado, ou seja, como a prova será introduzida dentro do processo. Diante disso, Vaz (2012) entende que podem ser adotados dois meios, o documental e o pericial.

Quanto ao meio de prova documental, o artigo 232 do Código de Processo Penal define como sendo “quaisquer escritos, instrumentos ou papéis, públicos ou particulares” (Brasil, 1941, não paginado). Além disso, para Lopes Júnior (2020), a prova não se limita a escritos, mas também a áudios, vídeos, fotografias e qualquer outro objeto móvel que possa ser incorporado no processo. Um exemplo de prova digital produzida por meio documental é a juntada no processo de arquivos audiovisuais, encontrados em um computador do autor de um delito.

Já o meio de prova pericial consiste em um trabalho técnico ou científico desenvolvido por pessoa dotada de conhecimento especializado, com o objetivo de obter um entendimento relevante sobre determinado fato, por meio da análise de pessoas ou coisas (Manzano, 2011, p. 08).

Neste aspecto, a produção da prova digital pelo meio pericial, ocorre por meio da realização de um trabalho técnico-científico prévio, pelo qual o perito, pessoa dotada de conhecimento especializado, irá analisar a prova obtida, visando verificar se esta pode ser considerada autentica e original, ou seja, se não sofreu manipulação e pode ter sua autoria associada a determinada pessoa.

Apesar da doutrina prever a existência dessas duas possibilidades de produção da prova digital, é importante ressaltar que esta trata-se de uma prova volátil, ou seja, de fácil alteração e manipulação (Vaz, 2012). Consequentemente, em virtude das peculiaridades que rodeiam a prova digital, é necessário que a incorporação desta no processo seja precedida da realização de perícia, buscando verificar sua autenticidade e validade. Além disso, não basta a realização de perícia prévia, mas sim de um procedimento, seja para obter a prova, armazená-la, periciá-la, preservá-la e descartá-la, ou seja, é preciso que haja uma cadeia de custódia da prova digital.

A cadeia de custódia, foi adicionada no Código de Processo Penal pela Lei 13.964/2019, que passou a vigorar em 2020. Os artigos 158-A e seguintes do referido diploma legal, disciplinam o que é a cadeia de custódia (a qual pode, em síntese, ser considerada como o histórico da prova), bem como as etapas a serem observadas naquele procedimento, visando a preservação da prova (Brasil, 2019).

Contudo, da leitura dos dispositivos que tratam do instituto da cadeia de custódia, é possível perceber que o legislador foi omisso sobre a forma de realização da cadeia de custódia de provas digitais, uma vez que os artigos do Código de Processo Penal que tratam do tema somente disciplinam as formalidades a serem adotadas na preservação de provas físicas, químicas e biológicas (Brasil, 1941).

Ocorre que, o procedimento a ser observado para a cadeia de custódia das provas digitais, não pode ser o mesmo do utilizado em provas físicas, químicas e biológicas, considerando as peculiaridades da prova digital, em especial sua volatilidade e fácil manipulação. Como exemplo, cita-se o artigo 158-B, inciso IV, do Código de Processo Penal, que dispõe sobre o acondicionamento de provas. Tal artigo, apenas menciona que o vestígio coletado deverá ser embalado, de forma individualizada, respeitando as suas características físico, químicas e biológicas, nada dizendo sobre a prova digital (Brasil, 1941).

Portanto, verifica-se a necessidade de perícia para a utilização da prova digital no processo penal, uma vez que o meio documental não é capaz de garantir a autenticidade da prova, considerando a possibilidade de tal prova ter sido manipulada. E mais, além da juntada de uma prova digital necessitar ser precedida da realização de perícia, deverá haver a observância da cadeia de custódia daquela prova, atentando-se para as peculiaridades desta, visando preservá-la e conhecer seu histórico, desde a sua coleta até o seu descarte. Sendo assim, diante das peculiaridades da prova digital, torna-se imprescindível saber como deve ser realizada a cadeia de custódia nestes casos.

4 A CADEIA DE CUSTÓDIA DA PROVA PENAL DIGITAL

Diante de uma breve análise sobre a evolução da tecnologia e seu impacto no direito criminal, bem como por meio do estudo da prova, destacando suas principais finalidades, regras e importância para o processo penal brasileiro e, por fim, com o estudo da prova digital, será possível compreender o instituto da cadeia de custódia, bem como buscar saber quais são as etapas necessárias para preservação da autenticidade e integridade da prova digital e os desafios a serem enfrentados para concretização destas etapas, a fim de evitar a sua quebra.

4.1 NOÇÕES INTRODUTÓRIAS DA CADEIA DE CUSTÓDIA: CONCEITO E SUA IMPORTÂNCIA PARA A PERSECUÇÃO PENAL

Na noite de 12 de julho de 1994, em um condomínio de luxo em Los Angeles, foram encontradas as vítimas Nicole Brown e Ronald Golman, assassinados brutalmente. A partir daquela noite foi dado início as investigações e, em seguida, ao processo e julgamento que perdurou por oito meses, tornando-se um dos juris mais longos e conhecidos dos Estados Unidos, a ponto de se tornar tema de série americana (The People VS O. J. Simpson, 2016).

No início das investigações, os vestígios colhidos apontavam a autoria criminosa para O. J. Simpson, famoso ex-jogador de futebol americano e ex-marido de Nicole. Isso porque, foram encontrados: fios de cabelo do réu na cena do crime, inclusive na blusa da vítima Ronald Golman; uma luva com sangue das vítimas e também do acusado; o sangue da vítima Nicole na meia do acusado; sem falar dos inúmeros registros de ocorrência que Nicole fez contra O. J. Simpson quando ainda eram casados (The People VS O. J. Simpson, 2016).

Diante destas provas, no início do julgamento a promotoria tinha o caso como ganho ao acusar O. J. Simpson como sendo o autor dos crimes de homicídio. Ocorre que a defesa passou a questionar todas as evidências coletadas na cena do crime como estratégia para ganhar aquele júri. A partir de então, a defesa começou a questionar as luvas, demonstrando que elas não serviam nas mãos do réu, além disso, questionaram o fato de um dos policiais ter levado os sapatos do acusado, que conteriam vestígios do crime, para sua própria casa. Também, passaram a questionar quaisquer outros vestígios, tendo em vista que um dos policiais responsáveis pela

investigação era racista e tinha registros de violência contra pessoa negras, indicando que este policial poderia ter modificado a cena do crime a fim de incriminar O. J. Simpson (The People VS O. J. Simpson, 2016).

Por consequência, mesmo havendo provas que o indicavam como sendo o autor daqueles delitos, a defesa conseguiu a absolvição devido aos procedimentos incorretos no momento da coleta e destino dos vestígios (Machado, 2017). Afinal, existiram graves erros, tais como: a deficiência no isolamento do local do crime; a coleta de vestígios sem luvas e sem a devida documentação; a falta de técnica dos peritos e, até mesmo, a destinação incorreta dos vestígios, como é o caso dos sapatos de Simpson que foram levados para a casa de um dos policiais ao invés de ser preservado e encaminhado a um perito (Cunha, 2020).

Este é um exemplo real das graves consequências oriundas do descuido no manejo correto das provas, o que pode desencadear erros judiciários e impunidades. Em vista disso, fica evidente a importância de preservar a autenticidade e integridade da prova no processo penal, já que a "luta pela qualidade da decisão judicial passa pela melhor prova possível" (Lopes Júnior, 2020, p. 659).

Por prova autêntica, entende-se a certeza de que o vestígio localizado e coletado na cena do crime é o mesmo que se encontra no processo, isto é, a garantia de que não houve mutação durante a persecução penal (Cunha, 2020). Já por íntegra, trata-se da prova completa, ou seja, aquela que não sofreu qualquer tipo de supressão (Fuller, *et al*., 2020). Em suma, não basta que a prova seja fidedigna ao que foi localizado no local do crime, é preciso também que todo o vestígio seja levado ao processo e não apenas parte dele.

Assim, a fim de buscar a autenticidade e integridade da prova, Prado (2019) entende que é preciso respeitar dois princípios: o da mesmidade e o da desconfiança. Por mesmidade, entende-se que as provas encontradas no local do crime devem ser as mesmas que estão no processo e que serão utilizadas para a decisão judicial (Bautista, 2005). Ademais, para Lopes Júnior (2020), este princípio busca evitar que a pessoa seja julgada com base em partes selecionadas pela acusação:

> não raras as vezes, por diferentes filtros e manipulações feitas pelas autoridades que colhem/custodiam a prova, o que é trazido ao processo não obedece à exigência de mesmidade, senão que corresponde ao signo de "parte do", que constitui, em última análise "a outro" e não "ao mesmo". (Lopes Júnior, 2020, p. 657).

Sendo assim, verifica-se que este princípio também busca garantir que, tanto a acusação quanto a defesa, tenham acesso integral às provas, principalmente aquelas que são colhidas fora do processo, como é o caso dos vestígios encontrados na fase investigatória, tais como a interceptação telefônica, as periciais, entre outras.

Já o princípio da desconfiança, exige que a prova sempre seja submetida a um processo de acreditação, não podendo ser preestabelecida como autêntica (Prado, 2019). Deste modo, é preciso que qualquer prova incluída no processo passe por um procedimento de valoração, a fim de saber todo o caminho que ela percorreu desde a sua coleta e, deste modo, poder aferir se ela é autêntica e íntegra ou se sofreu alterações ou supressões. Em relação a este princípio, Rosa e Lopes Júnior entendem que:

> quer se impedir a manipulação indevida da prova com o propósito de incriminar (ou isentar) alguém de responsabilidade, com vistas de obter melhor qualidade da decisão judicial e impedir uma decisão injusta. Mas o fundamento vai além: não se limita a perquirir a boa-fé ou má-fé dos agentes policiais/estatais, mas sim de objetivamente definir um procedimento que garanta e acredite a prova independente da problemática em torno do elemento subjetivo do agente. A discussão acerca da subjetividade deve dar lugar a critérios objetivos, empiricamente comprováveis, que independem da prova da má-fé ou bondade e lisura do agente estatal (Lopes Júnior; Rosa, 2015, não paginado).

Diante disso, o princípio da desconfiança não significa que haja má-fé dos agentes responsáveis pelo processo de coleta e manuseio da prova, mas sim que sempre deve-se observar critérios objetivos de verificação, a fim de que se possa valorar a prova com clareza. É neste cenário que surge a necessidade da utilização da cadeia de custódia,

a qual tem por objetivo garantir a autenticidade e integridade da prova, por meio do respeito aos princípios da mesmidade e da desconfiança.

Para melhor compreensão deste instituto, primeiramente, é preciso analisar o significado da expressão cadeia de custódia. Para Bautista (2005, não paginado), “cadeia é a continuidade dos acontecimentos e, continuidade é o que dura, funciona, se faz ou se estende sem interrupções; [já] custódia é a ação e o efeito de custodiar, e custodiar é guardar com cuidado e vigilância”.

Diante disso, verifica-se que a cadeia de custódia é um procedimento regrado e formalizado, que deve ser seguido e documentado de forma cronológica, desde a localização do vestígio até o seu descarte, a fim de possibilitar que seja admitido como prova no processo penal e possa ser valorado pelo órgão julgador (Lopes Júnior,

2020). Deste modo, a cadeia de custódia é um instrumento garantidor da autenticidade e integridade da prova, já que a protege de interferências internas e externas, assegurando que não haja supressões ou alterações daquilo que foi coletado (Lima, 2020). Neste sentido, também entende Badaró:

> Trata-se, portanto de um procedimento de documentação ininterrupta, desde o encontro da fonte de prova, até a sua juntada no processo, certificando onde, como e sob a custódia de pessoas e órgãos foram mantidos tais traços, vestígios ou coisas, que interessem à reconstrução histórica dos fatos no processo, com a finalidade de garantia sua identidade, a integridade e autenticidade (Badaró, 2017, p. 69).

Ademais, Fuller (2020, *et. al*., p. 189), aponta que a cadeia de custódia se trata de uma "norma geral de direito probatório", isso porque, ela não se limita à prova pericial, devendo ser utilizada também nos métodos ocultos de investigação, ou seja, aqueles que ocorrem sem a ciência do investigado/acusado, tais como a interceptação telefônica. Nessa perspectiva, Prado (2014) também entende que é necessária a aplicação da cadeia de custódia nos vestígios digitais, em virtude da facilidade de manipulação desta fonte de prova:

> a rede de garantias constitucionais formada para assegurar o axioma *nulla pena sine probatione* estaria em risco se desconsiderasse a possibilidade de manipulação dos suportes, em regra digitais, que recepcionam o resultado das diligências executadas com base em interceptações telefônicas, de *e-mails*, ambientais, infiltrações de policiais e colaboração premiada. E neste contexto, a preservação das fontes de prova é concebida como remédio jurídico-processual contra o desiquilíbrio inquisitorial, caracterizado pela seleção e uso arbitrário de elementos pelas agências repressivas (Prado, 2014, p. 75).

Justamente por isto, é que Badaró (2018, p. 385) entende ser a tarefa mais difícil do processo penal "a reconstrução histórica dos fatos, de acordo com as regras legais que disciplinam a investigação, a admissão, a produção e a valoração da prova". Logo, nota-se a imprescindibilidade da cadeia de custódia, já que o respeito a todas as etapas previstas em lei e a devida documentação cronológica, torna o processo penal mais democrático, isto é, um processo de respeito às garantias constitucionais e de combate às provas ilícitas (Jezler Junior; Eschiletti, 2017). De igual forma, Pacelli (2021, p. 547) entende que a cadeia de custódia possui a finalidade de:

> garantir a lisura e validade das provas que serão valoradas pelo julgador, maximizando-se o devido processo legal, sob duplo vetor: a) tanto sob a ótica da necessária apuração dos fatos na sua maior inteireza; b) como também

> para permitir o exercício da ampla defesa e do contraditório a partir de provas e indícios que sejam considerados como válidos à luz do ordenamento jurídico.

Em suma, verifica-se que o instituto da cadeia de custódia trata-se de um procedimento a ser obrigatoriamente aplicado sob qualquer vestígio encontrado, desde a sua descoberta, preservação, manuseio, até seu descarte, a fim de buscar a sua integridade e autenticidade, possibilitando chegar o mais próximo da verdade real e reduzir erros judiciários, que podem custar a liberdade ou impunidade de alguém. Além disso, também se refere à documentação cronológica das provas introduzidas no processo, possibilitando às partes averiguar sua legalidade no processo, cumprindo desta forma com o devido processo legal.

A discussão quanto a cadeia de custódia no Brasil não é recente, a exemplo disso, destaca-se o HC 160.662/RJ, julgado pela 6ª Turma do Superior Tribunal de Justiça, ainda no ano de 2014 (Brasil, 2014). No caso, durante as investigações referentes a operação Negócio da China foi determinada a interceptação telefônica, porém, parte desta interceptação foi perdida e os áudios não foram disponibilizados, o que gerou a descontinuidade das conversas. Diante disso, o STJ reconheceu a quebra da cadeia de custódia e, consequentemente, considerou nulas as provas produzidas a partir da interceptação telefônica, determinando a sua exclusão do processo, ao entender pela imprescindibilidade da preservação da integridade da prova (Lima, 2020). Além disso, para Badaró e Matida (2021), o reconhecimento da importância da cadeia de custódia da prova penal, no Brasil, ocorreu justamente a partir desta decisão.

Além disso, o Código de Processo Penal, ainda que de forma insuficiente, já previa alguns dispositivos referentes à cadeia de custódia, como é o caso do artigo 6º, inciso I, incluído no ano de 1994, e o artigo 169, e seu parágrafo único, incluídos no ano de 1973 e 1994, respectivamente. Estes artigos estabelecem que a autoridade policial deve tomar providências para preservar o local do crime até a chegada dos peritos e, estes, devem registrar no laudo qualquer alteração do estado das coisas, bem como a consequência dessas alterações (Brasil, 1941).

Ademais, em 2014, foi publicada a Portaria 82/2014, da Secretaria Nacional de Segurança Pública, a qual prevê quais os procedimentos a serem observados no tocante à cadeia de custódia de vestígios (Lima, 2020). Porém, somente em 2019,

com o advento da Lei Anticrime nº. 13.964/2019, é que este instituto foi inserido expressamente no Código de Processo Penal, junto ao capítulo do exame de corpo de delito, nos artigos 158-A ao 158-F (Brasil, 2019).

Foi a partir desta positivação que, felizmente, a cadeia de custódia ganhou maior ênfase no Brasil, sendo considerada por Lopes Júnior (2020, p. 650) “uma grande evolução para a qualidade epistêmica e a própria credibilidade da prova”. Além disso, Lima (2020, p. 255-256) acredita que:

> aquilo que à primeira vista pode parecer uma formalidade, uma medida meramente protocolar, consiste em relacionar e apor lacres aos objetos apreendidos, traduz, na realidade, em verdadeira garantia documental da cronologia dos fatos investigados pelo Estado, resguardando sua fiabilidade, visando garantir, em última análise, o pleno exercício do contraditório e da ampla defesa. [...] Esses dispositivos deixam transparecer que, doravante, não haverá mais espaço para admissão acrítica e cega das conclusões firmadas em laudos periciais, nem tampouco assertivas no sentido de que se presume a legitimidade dos atos praticados pelo Poder Público, pois a ordem jurídica convoca a jurisdição ao exame da legalidade da atividade anterior, preparatória, indagando sobre a estrita legalidade da obtenção e preservação do meio de prova.

No entanto, para que as suas finalidades sejam concretizadas, este instituto precisa ser aperfeiçoado, já que contém lacunas. Uma delas é a falta de previsão das etapas da cadeia de custódia quanto ao vestígio eletrônico ou digital (Matida, 2020). Diante disso, considerando que a tecnologia está cada vez mais presente, seja na prática de crimes, seja nos meios utilizados para investigação, faz-se necessária a previsão de como deve ser realizada a cadeia de custódia das provas digitais. Contudo, antes de buscar respostas para esta lacuna, é preciso compreender melhor a cadeia de custódia, por meio do estudo daquilo que já está positivado em lei.

4.2 ANÁLISE DA PREVISÃO LEGAL QUANTO A CADEIA DE CUSTÓDIA E A SUA QUEBRA

Após breve compreensão sobre o que se refere a cadeia de custódia, inclusive sobre sua finalidade e relevância para a persecução penal, passar-se-á a análise dos dispositivos legais sobre o assunto, em especial os artigos 158-A ao 158-F do Código de Processo Penal e a Portaria 82/2014 da Secretaria Nacional de Segurança Pública, a fim de que seja possível conhecer e entender quais as regras vigentes atualmente. Em seguida, também será feita uma análise quanto a quebra da cadeia de custódia,

com intuito de compreender quais as consequências da violação destes dispositivos legais.

4.2.1 O conceito e as etapas da cadeia de custódia trazidos pela Lei Anticrime n.º 13.964/19

Inicialmente, importante destacar que os artigos introduzidos no Código de Processo Penal pela Lei Anticrime se espelharam na Portaria 82/2014 da Secretaria Nacional de Segurança Pública, afinal esta traz regramento quanto ao conceito e as etapas da cadeia de custódia, assim como os artigos 158-A a 158-F do CPP, inclusive, as etapas mencionadas na Portaria são quase as mesmas previstas no Código (Lima, 2020). O primeiro artigo que trata sobre o tema, traz o conceito legal da cadeia de custódia, bem como o conceito de vestígio:

> Art. 158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.
> (...)
> § 3º Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal (Brasil, 2019, não paginado).

Diante disso, nota-se que a cadeia de custódia recai sobre o vestígio, o qual trata-se de qualquer objeto, mancha, marca, rastro ou sinal, encontrado no local da infração penal, podendo ser perceptível (percebido pelos sentidos humanos) ou latente (invisível ou oculto que necessita de técnicas para sua percepção) (Cunha, 2020). Além disso, os vestígios podem ser materiais, tais como uma faca ou munição, ou imateriais, entendendo-se por aqueles registrados eletronicamente (Machado, 2020).

Em relação a esta última classificação, Badaró (2017) destaca que a cadeia de custódia deve ser considerada mais ampla, devendo ser aplicada a qualquer fonte de prova real, ou seja, a qualquer objeto, seja ele um vestígio material ou imaterial. Contudo, para Matida (2020), o conceito trazido pelo Código de Processo Penal é limitado, já que não faz menção aos vestígios imateriais. Dessa forma, verifica-se que o conceito legal precisa evoluir e se adequar a realidade atual, já que os vestígios eletrônicos e digitais são cada vez mais recorrentes dentro da área criminal (Machado, 2020).

Após trazer o conceito, o artigo 158-A, § 1º, do Código de Processo Penal traz o momento em que se dá início à cadeia de custódia, podendo ocorrer em três hipóteses, são elas: i) com a preservação do local de crime; ii) com procedimentos policiais; ou iii) com procedimentos periciais (Brasil, 2019).

Primeiramente, quanto ao início da cadeia de custódia por meio da preservação, consiste em manter o estado original do local do crime e das coisas encontradas nele, até a chegada dos peritos criminais. Ademais, a Portaria 82/2014 do SENASP entende que o local do crime é composto por três áreas: imediata, mediata e relacionada. A área imediata é onde ocorreu o fato investigado, por este motivo, provavelmente é a região que concentra maior número de vestígios. Por outro lado, a área mediata consiste nos arredores da imediata, ou seja, o grande ambiente externo, local em que também podem ser encontrados vestígios. Por fim, a área relacionada é qualquer ligação geográfica com o local do crime que possa ter algum vestígio ou informação relacionada ao fato (Lima, 2020).

Já em relação ao início da cadeia de custódia por meio do procedimento policial, ocorre quando agentes policiais localizam vestígios relacionados a um delito, seja durante patrulhamento ou durante a própria investigação da infração penal. Por outro lado, a cadeia de custódia inicia pelo procedimento pericial, quando o perito, ao exercer o seu trabalho técnico, localiza vestígios de um fato ilícito (Lima, 2020).

Posto isso, percebe-se que a cadeia de custódia pode iniciar antes mesmo da perícia criminal, seja com a primeira autoridade a chegar no local do crime ou a encontrar os primeiros vestígios, a qual ficará responsável pela sua preservação (Cunha, 2020). Ademais, a Portaria 82/2014, define como agente público “todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer forma de investidura ou vínculo, mandato, cargo, emprego ou função pública” (Brasil, 2014, não paginado).

Em seguida, o Código de Processo Penal traz o artigo 158-B, o qual elenca todas as etapas da cadeia de custódia, cronologicamente, sendo elas: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte (Brasil, 2019).

A etapa inicial é a do reconhecimento, a qual consiste no “ato de designar um elemento como de potencial interesse para a produção da prova pericial” (Brasil, 2019, não paginado), ou seja, é o momento em que se analisa o local do crime ou objetos, a fim de localizar quais são os vestígios ligados à infração penal investigada.

Após o reconhecimento, passa-se a etapa do isolamento, o qual consiste na preservação do local do crime, incluindo a área imediata, mediata e relacionada, a fim de evitar a alteração do estado das coisas (Brasil, 2019), isto é, impedir que os vestígios rastreados sejam contaminados (Cunha, 2020). Ademais, importante destacar que o artigo 158-C, §2º, do CPP, proíbe a entrada no local isolado, bem como a retirada dos vestígios sem a liberação pelo perito oficial, considerando tais atos como crime de fraude processual (Brasil, 2019).

Em seguida, com os vestígios localizados e protegidos, passa-se à etapa de fixação, consistente na “descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito” (Brasil, 2019, não paginado). Além disso, destaca-se que esta descrição deve ser realizada por perito responsável pelo atendimento, o qual deverá confeccionar o laudo, adicionando todas as anotações, facultando ainda, a utilização de fotografias, croquis e filmagens a fim de facilitar o trabalho do perito (Brasil, 2019).

Depois passa-se a etapa da coleta, quando os vestígios são recolhidos do local para serem enviados ao órgão pericial (Lima, 2019). Além disso, o artigo 158-C, *caput*, do CPP, estabelece que a coleta deve ser realizada preferencialmente por perito oficial (Brasil, 2019). Diante desta previsão, entende-se que a coleta por perito não oficial é uma exceção, podendo atuar somente na impossibilidade daquele (Lima, 2020). Também, importante destacar que a Portaria 82/2014 do SENASP exige ainda dois requisitos: a obrigatoriedade de utilização de equipamentos de proteção individual (EPI) e a numeração de maneira individualizada de cada vestígio (Brasil, 2014).

Quanto ao procedimento a ser adotado no momento da coleta, dependerá do tipo de vestígio, devendo o perito se basear em manuais específicos da prática pericial (Cunha, 2020). Inclusive, o profissional deve coletar amostra suficiente, haja vista que “a insuficiência da amostra e a falta de fornecimentos de comparação são os erros mais comuns” (Lima, 2020, p. 262). Por fim, Machado (2017) destaca a importância de evitar a contaminação no momento da coleta, a fim de manter a qualidade da prova.

Após a coleta, passa-se para a etapa do acondicionamento, “procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas” (Brasil, 2019, não paginado), ou seja, é o procedimento utilizado para manter o vestígio protegido e

identificado, evitando a sua perca ou contaminação no momento em que for retirado do local e transportado.

Ademais, quanto ao recipiente a ser utilizado para o acondicionamento, dependerá da natureza do material, podendo ser utilizados envelopes, caixas, frascos, ou outros meios, desde que seja apropriado para aquele tipo de vestígio, devidamente selado com lacres e identificado individualmente por meio de numeração (Brasil, 2014). Ainda, quanto a identificação, analisando conjuntamente o Código de Processo Penal e a Portaria do SENASP, exige-se: anotação da data, hora e local da coleta e acondicionamento; especificação e quantidade do vestígio; nome e identificação do agente e do órgão coletor, do órgão de destino, e do agente recebedor, com protocolo de recebimento, assinatura e rubrica; e, por fim, o número de procedimento e respectiva unidade de polícia judiciária a que o vestígio estiver vinculado (Brasil, 2014).

Com o acondicionamento do que foi coletado, possibilita-se a realização do transporte, próxima etapa a ser observada, a qual consiste em transportar o vestígio de um local para o outro, ou seja, do local da coleta, até o órgão que realizará a perícia. Para tanto, deve-se sempre utilizar o meio mais adequado de transporte para cada tipo de vestígio, a fim de garantir a manutenção de suas características originais e do controle de sua posse (Brasil, 2019). Logo, nada serve o acondicionamento do vestígio, se este não for destinado ao local correto, ou se o transporte utilizado não for o adequado para sua preservação.

Realizado o transporte até o órgão pericial, passa-se à etapa do recebimento do vestígio, tratando-se do “ato formal de transferência da posse do vestígio” (Brasil, 2019, não paginado), isto é, o momento em que o vestígio chega no órgão pericial e é entregue aos profissionais responsáveis pela perícia. Além disso, o Código de Processo Penal exige a documentação desta entrega, devendo conter o “número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu” (Brasil, 2019).

Em seguida, passa-se a etapa do processamento, o qual consiste no exame pericial em si, realizado pelo perito oficial (Brasil, 2019, não paginado). Para dar início à perícia, é necessário o rompimento do lacre, ato que só pode ser realizado pelo próprio perito ou por pessoa autorizada por este, ademais, toda vez que o lacre é rompido, deve-se fazer a devida documentação, indicando a hora, local, finalidade, a

pessoa responsável, bem como as informações do novo lacre utilizado (Dezem; Souza, 2020).

Após o rompimento do lacre, o perito deve realizar a perícia do vestígio, utilizando-se da metodologia adequado às características biológicas, físicas e químicas do vestígio e, ao final, confeccionar o laudo (Brasil, 2019). Por fim, cumpre mencionar o Manual de Procedimento Operacional Padrão, do SENASP, o qual prevê quais os procedimentos a serem seguidos para realização de cada tipo de perícia (Lima, 2020).

Findada a perícia, a próxima etapa é o armazenamento, consistente no procedimento de guardar o vestígio em condições adequadas, a fim de mantê-lo preservado até o seu transporte ou descarte (Brasil, 2019). Além disso, dependendo do tipo de material examinado, parte deste deverá ser guardado, possibilitando a realização de contraperícia, caso haja impugnação do laudo anterior (Cunha, 2020). Ademais, para ser possível a realização desta etapa, o órgão pericial deve conter "espaço adequado com condições técnicas específicas capazes de preservar as características do material a ser processado, evitando contaminação, vazamento e adulteração" (Cunha, 2020, p. 190).

Finalmente, a última etapa consiste no descarte, isto é, no "procedimento referente à liberação do vestígio" (Brasil, 2019, não paginado). Assim, deve ser guardada apenas uma pequena quantidade necessária para eventual contraperícia e o restante deve ser descartado (Lima, 2020). Para o descarte, é necessário que haja autorização judicial, bem como a observância do procedimento específico a depender do tipo de objeto (Cunha, 2020), a exemplo disso, destacam-se as armas de fogo apreendidas, as quais, após a realização da perícia, só poderão ser descartadas com autorização judicial, e serão encaminhadas para o Comando do Exército, conforme disciplina o artigo 25 da Lei 10.826/03 (Estatuto do Desarmamento).

Por fim, o artigo 158-E do CPP exige que cada Instituto de Criminalística possua uma central de custódia, a qual terá a finalidade de guarda e controle dos vestígios. Assim, o material coletado deve ser levado até a central de custódia, onde ficará armazenado até a perícia, e, após a realização desta, o vestígio retornará para a central, onde permanecerá guardado até o seu descarte (Brasil, 2019).

Além disso, estas centrais devem "possuir serviços de protocolo, com local para conferência, recepção e devolução dos materiais e documentos" (Brasil, 2019, não paginado). Ademais, a fim de evitar qualquer alteração ou perda dos vestígios ali

armazenados, é preciso que o ambiente possua condições adequadas e que haja o controle da entrada e saída dos vestígios e das pessoas que tiverem acesso (Brasil, 2019).

Em suma, com o cumprimento de todas as etapas supramencionadas, é que se possibilitará o cumprimento da cadeia de custódia e, por conseguinte, a autenticidade e integridade da prova, chegando-se ao mais próximo possível da verdade real e da decisão justa.

Contudo, a Lei Anticrime deixou de prever quais seriam as consequências da quebra da cadeia de custódia, isto é, da violação de alguma destas etapas. Deste modo, para que haja o devido respeito a este instituto, é preciso que se estabeleçam os efeitos de sua violação, caso contrário, de nada servirá a regulamentação trazida pela referida lei. Por este motivo, é importante analisar qual o entendimento atual da doutrina e da jurisprudência quanto a este impasse.

4.2.2 As consequências da quebra da cadeia de custódia

A qualidade da decisão judicial depende da qualidade do material probatório utilizado no processo. É por este motivo que apenas a prova admitida poderá permanecer nos autos e ser valorada (Machado, 2020). Logo, a prova ilícita deve ser desentranhada do processo criminal, e a prova lícita será admitida e passará pelo juízo de valoração pelo magistrado.

A partir deste ponto, é que surgiram duas correntes doutrinárias referente ao efeito da quebra da cadeia de custódia, a primeira entende que a prova seria ilícita, e, portanto, deveria ser excluída do processo, inclusive, as derivadas dela. Por outro lado, a segunda corrente entende que a prova seria lícita, logo, admitida no processo, devendo o vício ser resolvido no momento da sua valoração, levando em consideração o grau de autenticidade (Machado, 2020).

Quanto à primeira corrente (ilicitude), Lopes Júnior (2020) defende que a quebra da cadeia de custódia ocasiona a inutilização da prova, sendo proibida sua valoração no processo, devendo esta e todas as derivadas dela, ser excluídas dos autos. Além disso, Lopes Júnior (2020) destaca que não se pode confundir a teoria da ilicitude, aplicada neste caso, com a teoria da nulidade, isso porque, apesar de ambas figurarem no campo da ilicitude, não se aplica na prova ilícita a preclusão ou prejuízo,

ou seja, não há prazo para alegar a ilicitude de uma prova, nem mesmo há necessidade de provar o prejuízo causado por esta.

Neste mesmo sentido, Matida (2020) critica a admissibilidade de provas não confiáveis no processo, ao entender que o juiz brasileiro ainda está muito ligado ao sistema inquisitório, e, por este motivo, muitas vezes não respeita as ferramentas técnicas utilizadas para saber como se deram os fatos, aplicando termos retóricos como a verdade real e o livre convencimento, sem falar da inclinação pelas teses da acusação.

Diante disso, a autora entende que não há razões para acreditar que o "juiz brasileiro saberá ser firme quanto à debilidade probatória de elementos relevantes, porém não confiáveis" (Matida, 2020, não paginado). Ou seja, admitir uma prova não confiável pode pôr em risco o sistema acusatório e, consequentemente, também a decisão imparcial, já que o juiz, no momento da valoração da prova, se importará mais com a sua relevância no processo, do que com possíveis manipulações ou supressões.

Já quanto a segunda corrente, Lima (2020) entende que eventual falha na cadeia de custódia, por si só, não gera automaticamente a ilicitude/invalidade da prova. Assim, esta prova deve ser admitida no processo, possibilitando a valoração pelo juiz, o qual conferirá maior ou menor credibilidade. Como exemplo, o autor destaca a ausência do lacre no recipiente que armazena o vestígio, o que não geraria, automaticamente, a ilicitude da prova, devendo ser analisado no processo se a ausência de lacre gerou ou não alguma violação do conteúdo deste vestígio.

Cunha (2020) também defende esta corrente, ao alegar que a prova não deve ser descartada, mas sim valorada, possibilitando que as partes possam questionar a autenticidade da prova. Inclusive, Badaró (2017) segue neste mesmo sentido, ao entender pela admissibilidade da prova decorrente da irregularidade da cadeia de custódia, pois assim, "haverá uma inegável necessidade de reforço justificativo demonstrando o porquê ser possível confiar na autenticidade e integridade de tal fonte" (Badaró, 2017, p. 536), ou seja, com a prova nos autos, possibilitar-se-á, tanto à acusação quanto à defesa, questioná-la, exigindo provas da sua autenticidade e integridade.

Já Dezem e Souza (2020), trazem posicionamento um pouco diverso, ao entenderem que a quebra da cadeia de custódia torna a prova nula, haja vista que o desrespeito às etapas, violam as normas do Código de Processo Penal, cabendo ao

órgão acusatório provar que não há prejuízo, afastando a nulidade. Ou seja, havendo quebra da cadeia de custódia da prova, ela será considerada nula e não poderá ser utilizada pelo juiz no momento de fundamentar a sua decisão, porém, caso a acusação demonstre que esta quebra não gerou prejuízo, afasta-se a nulidade e poderá ser valorada. Em relação a jurisprudência, também não há entendimento pacífico referente a quebra da cadeia de custódia, como exemplo disso, destacam-se os julgados controvertidos entre as Turmas do STJ.

No Agravo Regimental no Recurso Ordinário em Habeas Corpus 143.169/RJ, da 5ª Turma do STJ, filiou-se à primeira corrente doutrinária, ao reconhecer a inadmissibilidade da prova que violou a cadeia de custódia em virtude de sua ilicitude. No caso concreto, entendeu a Corte que a ausência de documentação das etapas de arrecadação, armazenamento e análise de arquivos digitais extraídos de computadores dos investigados, acarretou na quebra da cadeia de custódia da prova, ensejando a sua ilicitude, e, consequente, inadmissibilidade no processo, motivo pelo qual deveria ser determinado seu desentranhamento dos autos pelo juiz de primeiro grau (Brasil, 2021).

Já a 6ª Turma do STJ, no julgamento do Habeas Corpus 653.515, seguiu a segunda corrente doutrinária, ao entender que a quebra da cadeia de custódia não implica obrigatoriamente na nulidade da prova e em sua extirpação dos autos, cabendo ao juiz verificar se ela é confiável ou não no caso concreto, mediante a análise dos demais elementos de prova, os quais, em seu conjunto, permitirão concluir pela confiabilidade ou não da prova questionada. Logo, para esta corrente jurisprudencial, eventual desrespeito à cadeia de custódia não possui o condão de acarretar o desentranhamento da prova, visto que sua confiabilidade poderá ser auferida pela análise de outros elementos probatórios, decidindo o juiz, se for o caso, decretá-la nula ou retirá-la dos autos (Brasil, 2017). Em suma, diante desta lacuna legislativa, verifica-se que conforme os entendimentos da doutrina e dos tribunais, ainda não há pacificação quanto a quebra da cadeia de custódia, tanto em relação a sua ocorrência, quanto aos seus efeitos.

Assim, após uma análise geral sobre a cadeia de custódia, a fim de compreender os principais pontos, como a sua finalidade, suas etapas e as consequências da violação deste instituto, verifica-se notória a importância da cadeia de custódia para a qualidade da prova. Contudo, tanto o Provimento do SENASP quanto a Lei Anticrime, deixaram de prever quais seriam as etapas necessárias para

preservar a autenticidade e integridade de uma prova digital. Como visto anteriormente, esta espécie de prova possui características específicas, tais como a volatilidade, o que significa facilidade na perda ou alteração do material probatório. Além disso, a prova digital origina-se de vestígios imateriais, logo, não há um objeto físico, mas sim um dado digital. Sendo assim, a fim de fortalecer a técnica do sistema probatório, faz-se necessário estabelecer quais são as etapas da cadeia de custódia da prova digital.

4.3 AS ETAPAS E OS DESAFIOS PARA PRESERVAÇÃO DA CADEIA DE CUSTÓDIA DA PROVA DIGITAL

Diante de uma sociedade informatizada, é comum, ao analisar procedimentos investigatórios e processos criminais, encontrar no seu material probatório vestígios digitais, tais como mídias de computadores e celulares, interceptações telefônicas e, até mesmo, dados retirados diretamente da rede, como os sites, redes sociais e armazenamentos em nuvem. Em virtude da grande incidência de vestígios digitais usados como prova no processo penal, é que se justifica a preocupação com a sua qualidade, mostrando-se essencial preservar sua autenticidade e integridade (Machado, 2022).

Assim, como já destacado, a cadeia de custódia é um instrumento utilizado justamente para esta finalidade. Contudo, o impasse reside na inexistência de lei que estabeleça as etapas da cadeia de custódia da prova digital, e não só isso, mas também a falta de conhecimento e treinamento técnico das autoridades que atuam ao longo da persecução penal.

Apesar do Provimento do SENASP e da Lei Anticrime estabelecerem as etapas da cadeia de custódia, estas mostram-se inaplicáveis ao vestígio digital. Isso porque, ao fazer uma análise dos dispositivos legais, nota-se que este instituto recai apenas sobre o vestígio material, caracterizado por ser bruto e visível ou latente, possuindo aspectos opostos em relação ao vestígio imaterial/digital, caracterizado por ser incorpóreo e intangível.

> A noção conceitual externada pelo legislador ordinário, de igual forma, restringe a caracterização do eventual elemento a ser sujeito à cadeia de custódia probatória àqueles passíveis de posse ou manuseio, ou seja, insere enquanto características primordiais do elemento sua sujeição à locomoção e seu aspecto material, exigindo, ao que parece ser, que seja um elemento

> que possa ser tocado, movimentado e percebido pelos sentidos, sobretudo o tato (Duarte, 2020, p. 26).

No mesmo sentido, Parodi (2020) destaca que os dispositivos legais sobre a matéria, foram criados pensando unicamente no vestígio físico/material, vez que o legislador deixou de considerar as peculiaridades da prova digital. Como prova disso, basta analisar as etapas previstas no Código de Processo Penal. A exemplo, destaca-se as etapas de coleta, acondicionamento e transporte, em que a prova material é recolhida pela autoridade, colocada dentro de uma embalagem adequada à suas características físicas, químicas e biológicas, e transportada até o órgão pericial por meio de um transporte adequado. Porém, suponha-se que a prova seja digital, como a autoridade fará para coletar estes dados? É necessário a atuação de pessoa com capacidade técnica em informática? Deverá, a autoridade, recolher os dispositivos ou fazer cópia das mídias no local? Onde armazenar os dados encontrados? Como preservar a evidência digital para que não haja alterações?

Diante deste exemplo, nota-se que é incabível e insuficiente a aplicação das etapas da cadeia de custódia trazidas pela Lei Anticrime quanto aos vestígios digitais. Assim, diante desta lacuna legislativa, verifica-se que ainda não há uma resposta concreta para este impasse. No entanto, por meio de um estudo conjunto da doutrina, da jurisprudência e da norma técnica ABNT NBR ISO/IEC 27037 2013, será possível estabelecer quais as etapas devem ser observadas quanto ao vestígio digital.

4.3.1 As etapas da cadeia de custódia da prova digital

Apesar de inexistir lei brasileira que preveja as etapas da cadeia de custódia da prova digital, há uma norma técnica, a ABNT NBR ISO/IEC 27037 de 2013, a qual estabelece as etapas de identificação, coleta, aquisição (cópia) e preservação da evidência digital. No entanto, conforme a própria norma prevê, estas etapas referem-se apenas ao processo inicial de manuseio da evidência digital, ou seja, somente entre o momento da localização do vestígio até a coleta e preservação, não prevendo as etapas posteriores que se seguem até a inserção desta evidência no processo e posterior arquivamento/descarte (Brasil, 2013). Além disso, importante destacar que se trata de uma norma técnica, logo, o objetivo é estabelecer recomendações de como manusear um vestígio digital, e não propriamente estabelecer as etapas da cadeia de custódia. Inclusive, não se trata de um documento público, já que é necessário adquiri-

lo para ter acesso, além de não ter a mesma força impositiva que tem o Código de Processo Penal (Almas, 2021).

Diante disso, percebe-se que a referida norma não é suficiente para suprir a lacuna legislativa, sendo necessário uma análise também da doutrina. Assim, importante destacar a obra de Souza, Carvalho e Munhoz (2023), a qual prevê outros procedimentos além daqueles previstos pela ABNT NBR ISO/IEC 27037. Para os autores, as etapas consistem no: i) isolamento; ii) coleta; iii) preservação, iv) roteiro, v) perícia técnica e vi) documentação da prova.

Outrossim, cabe analisar também a obra de Marshall (2008), a qual estabelece quase as mesmas etapas previstas na norma técnica e na obra acima mencionada, porém, possui algumas nomenclaturas distintas. Para o autor as etapas são as seguintes: i) recolha, ou seja, a identificação e coleta do vestígio; ii) exame, consistente na realização de cópia das evidências coletadas; iii) autenticação, que nada mais é que a fase da preservação; iv) armazenamento; v) análise, isto é, a realização da perícia; vi) relatório, ou seja, a documentação de todo processo percorrido e, por fim; vii) destruição.

Em suma, por meio da análise da norma técnica e das obras supramencionadas, conclui-se que as etapas previstas são: i) isolamento, ii) identificação, iii) coleta, iv) transporte, v) cópia/aquisição, vi) arquivamento/preservação, vii) perícia/análise, viii) documentação/relatório e ix) destruição.

Porém, antes da análise de cada uma destas etapas, será necessário compreender dois pontos importante. O primeiro deles é verificar se há necessidade de autorização judicial para realização do procedimento e, o segundo, refere-se a estabelecer quem possui competência para realizar estas etapas.

Quanto à autorização judicial, a ABNT NBR ISO/IEC 27037, considera impraticável a coleta e aquisição do vestígio, caso não haja autorização legal para tanto (Brasil, 2023). Ainda, importante destacar a Lei 12.965/2014 (Marco Civil da Internet), a qual prevê no seu artigo 13, § 5º, que quaisquer registros de conexão à internet, só serão disponibilizado após autorização judicial (Brasil, 2014). Além disso, o artigo 5º, inciso XII, da Constituição Federal, garante a inviolabilidade do sigilo de dados e comunicações telefônicas, permitindo sua violação somente nos casos de investigação criminal ou instrução processual penal, desde que haja ordem judicial (Brasil, 1988).

Ademais, em relação a referida garantia constitucional, o STF entendia que esta proteção era aplicada somente em relação ao conteúdo dos dados e das comunicações telefônicas, não se estendendo aos dados registrais. Exemplificando, no julgado do HC nº 91.867/PA, a Corte Superior entendeu que o acesso direto dos dados do celular, sem autorização, não violaria a Constituição Federal (Brasil, 2012). Contudo, com o avanço da tecnologia, os celulares passaram a ter acesso à internet e, por este motivo, o STJ passou a adotar entendimento diverso do STF, como é o caso do RHC nº 51.351/RO, julgado pela 6ª Turma, ainda no ano de 2014, o qual entendeu ser necessária prévia autorização judicial para colher os dados armazenados em celulares (Brasil, 2016). Assim, com o passar do tempo e do avanço tecnológico, o STF reconheceu a ocorrência de mutação constitucional no HC nº 168.052/SP, julgado em 2019, passando a reconhecer a ilegalidade no acesso de dados em aparelhos celulares, sem autorização judicial (Brasil, 2020).

Assim, nota-se que há necessidade de autorização judicial para coleta e manuseio dos vestígios digitais, a fim de evitar a violação de direitos constitucionais, tais como a privacidade e a intimidade, o que pode levar a ilicitude da prova e, consequentemente, inutilidade desta no processo.

Dito isso, importante também definir quem possui capacidade para realizar as etapas da cadeia de custódia. Para a ABNT NBR ISO/IEC 27037, a pessoa capaz para realização do manuseio da evidencia digital é o Primeiro Interventor da Evidência Digital (DEFR), isto é, a “pessoa autorizada, treinada e qualificada para agir primeiro no local do incidente, na execução da coleta e aquisição de evidência digital, responsabilizando-se pelo seu manuseio” (Brasil, 2013, p. 2). Logo, a referida norma técnica não exige a atuação de um perito para identificação, coleta e preservação de uma evidencia digital, bastando uma pessoa treinada e qualificada.

Para definir quem possui esta competência, a norma técnica traz uma tabela, com a descrição das habilidades, conscientizações e conhecimentos que a pessoa deve possuir, resumindo-a, a grosso modo, nas capacidades e habilidades em tecnologia da informação, com competência no uso geral da TI e administração dos mais diversos dispositivos eletrônicos e aplicativos, bem como da rede (Brasil, 2013).

O STJ já decidiu neste sentido, no julgado HC 762.844, em 2023, inclusive, fazendo menção a norma da ABNT. No caso, o Ministério Público teve acesso à dados armazenados em nuvem, relativos ao paciente, disponibilizados pela Apple por meio

de pen drive, tendo o Ministério Público transferidos os dados para um HD externo. Diante disso, a defesa impetrou Habeas Corpus, alegando a quebra da cadeia de custódia, uma vez que o vestígio não foi armazenado por perito oficial, mas sim por um perito do Centro de Apoio Operacional à Execução (CAEX), que presta auxílio ao Ministério Público. No entanto, o STJ reconheceu não haver a necessidade de perito oficial, sendo cabível a atuação do CAEX, uma vez que este presta auxílio técnico-jurídico ao Órgão Ministerial, além de que a coleta e armazenamento destes dados não exigem conhecimento ou habilidade especial:

> o servidor atua justamente no Laboratório de Computação Forense, setor incumbido da atividade de realizar extração, processamento e análise pericial de dados digitais e físicos, cujas 'atividades são pautadas em normas de órgãos nacionais e internacionais para tratamento e análise pericial dos vestígios digitais e/ou físicos, tais como: SWGDE, FISWG, SENASP, ABNT ISSO/IEC 27037, RFC 3227, entre outras.' Dessa forma, conforme já exposto, o auxílio prestado por servidor público do CAEX aos Promotores de Justiça na realização de trabalho que não exige nenhum conhecimento ou habilidade especial que justifique a obrigatoriedade de que seja realizado por perito oficial, durante a fase de investigação, é legalmente permitido e não gera qualquer irregularidade ou nulidade (Brasil, 2023, não paginado).

Diante o exposto, de acordo com a referida ABNT, bem como o entendimento da jurisprudência, verifica-se que no momento do manuseio da evidência digital, isto é, durante a sua identificação coleta e proteção, não é exigível um perito oficial, bastando a atuação de pessoa capacitada na área da TI, com treinamento e respeito às normas técnicas, exigindo-se perito oficial somente nos casos de maior complexidade, como no momento da realização da perícia. Em suma, após análise destes dois pontos importantes, se passará à análise individual de cada uma das etapas da cadeia de custódia da prova digital.

A primeira etapa é o isolamento, o qual consiste em isolar o local onde podem haver possíveis evidências digitais, a fim de evitar interferências, que podem ocasionar contaminações e manipulações dos vestígios (Souza; Munhoz; Carvalho, 2023). Para tanto, primeiro é necessário assumir o controle da área; determinar quem será o responsável pelo local; registrar quais as pessoas que tiveram acesso a área; documentar a cena por fotografias, desenhos ou vídeos; procurar informações importantes como senhas e PIN; e manter o dispositivo no estado em que se encontra, ou seja, se ligado, mantê-lo ligado, se desligado, mantê-lo desligado (Brasil, 2013). Além de isolar

o local, deve-se buscar a segurança das pessoas envolvidas, devendo considerar algumas questões, tais como, se os indivíduos investigados estão no local e se estão propensos à violência; se é possível evitar a passagem de transeuntes; se há armas no local; se a cena do incidente é segura; entre outros cuidados (Brasil, 2013).

Após isolar o local e mantê-lo seguro, passa-se à identificação, a qual consiste na pesquisa, reconhecimento e documentação do vestígio digital. Ou seja, nesta etapa, busca-se pesquisar e localizar onde podem estar armazenadas as possíveis evidencias digitais da infração penal investigada, realizando em seguida, a documentação dos resultados (Brasil, 2013). Além disso, para Marshall (2008), esta etapa refere-se ao procedimento de pré-visualização, consistente na identificação dos dispositivos que podem ser relevantes para a investigação, para posterior coleta.

Para tanto, primeiro é preciso verificar se a evidencia encontra-se na forma física ou lógica, isto é, se está armazenada em um dispositivo eletrônico, como o celular, ou representada apenas no formato virtual, como acontece com os dados contidos na nuvem. Além disso, caso haja evidencias armazenadas em meio físico, ainda deve-se averiguar se este dispositivo está ou não conectado na rede. Esta pesquisa inicial é imprescindível, uma vez que antes da coleta da evidencia digital, faz-se necessário tomar algumas medidas de segurança e realizar a devida documentação, sendo que a forma de armazenamento e a conexão ou não na rede, define como isso acontecerá (Brasil, 2013).

Assim, em relação aos dispositivos físicos não conectados na rede, estes englobam: i) os computadores, dispositivos autônomos que recebem, processam e armazenam dados; ii) os dispositivos periféricos, os quais são conectados aos computadores para aplicar seu funcionamento, tais como *webcams*, sistemas de GPS e dispositivos RFID (identificação de rádio frequência); e iii) as mídias de armazenamento digital, as quais referem-se a armazenamento de dados, com variação na capacidade de memória, tais como *pen drive*, CD, DVD e cartões de memória. Caso sejam encontrados algum destes dispositivos, devem ser tomadas as seguintes providências: identificar todos os computadores, periféricos e armazenamentos digitais que serão coletados; documentar a marca, o número de série e o número de licença; manter no estado em que se encontra, ou seja, se desligado mantê-lo desligado e se ligado mantê-lo ligado, a fim de evitar a alteração das evidências; caso esteja ligado, deve-se fotografar e documentar o que aparece na tela, bem como coletar carregadores e baterias, a fim de evitar a descarga e o desligamento do dispositivo (Brasil, 2013).

Por outro lado, em relação aos dispositivos físicos ligados na rede, tais como computadores de mesa, roteadores e dispositivos móveis, ou no caso de os dados estarem representados apenas no formato virtual, devem ser tomadas as seguintes providências: localizar e documentar todos os dispositivos que podem conter possíveis evidências, inclusive, localizar as suas embalagens originais, as quais podem conter informações importantes do dispositivo, como os códigos PIN e PUK (códigos de segurança); documentar o tipo, modelo, marca e número de série; documentar e coletar todos dispositivos móveis e itens acessórios, como carregadores e cartões de memória; manter os dispositivos no estado em que se encontram (ligado/desligado), a não ser que o dispositivo seja coletado somente em futuro indeterminado, caso em que se recomenda desliga-lo para minimizar os danos; verificar se estes dispositivos podem ser desconectados da rede ou não, uma vez que, a depender do caso, a desconexão pode gerar perda de potenciais evidências digitais; caso o dispositivo seja um sistema CFTV (circuito fechado de televisão), é preciso anotar o número, modelo, fabricação, configurações básicas e o local de armazenamento, bem como se estas câmeras estão em operação ativa; por fim, recomenda-se utilizar detectores de sinal rede sem fio, a fim de localizar dispositivos de rede sem fio que podem estar escondidos (Brasil, 2013).

Ainda, importante destacar que todo este procedimento inicial deve ser documentado, sendo que além das documentações exigidas acima, deve constar também quem e quando acessou as evidências, o motivo, bem como se houve alguma alteração de evidências (Machado, 2022).

Por fim, quando houver dispositivos físicos, é preciso guardá-los em uma embalagem adequada, levando em consideração suas características, bem como utilizar-se do lacre, a fim de assegurar a preservação do dispositivo até o momento da coleta dos dados. A exemplo disso, destaca-se a Gaiola de *Faraday*[13]*,* utilizada pelos peritos para isolar o celular, evitando qualquer comunicação externa. Contudo, importante destacar que nem sempre será possível evitar contaminações ou perdas antes da coleta, assim, caso o dispositivo seja corrompido, mesmo que se sigam as demais etapas corretamente, não será possível lhe atribuir segurança (Souza; Munhoz; Carvalho, 2023).

[13] “Uma Gaiola de Faraday é uma blindagem elétrica, ou seja, uma superfície condutora que envolve uma dada região do espaço e que pode, em certas situações, impedir a entrada de perturbações produzidas por campos elétricos e ou eletromagnéticos externos” (Neto, [s.d], não paginado).

Após isolar o local e mantê-lo seguro, bem como identificar onde podem estar armazenadas as possíveis evidências digitais, passa-se à etapa da coleta. Para Marshall (2008), esta etapa consiste na recolha dos dispositivos que possam conter potencial fonte de provas digitais. No mesmo sentido, a ABNT NBR ISO/IEC 27037 (2013), entende que a coleta se refere a remoção dos dispositivos do local em que se encontram, levando-os a um laboratório ou outro ambiente, para posterior aquisição (cópia) e análise (perícia).

Contudo, nem sempre será realizada a etapa da coleta, pois a depender do caso, a evidência não poderá ser retirada do local original, devendo passar direto para a etapa da aquisição, a qual consiste na cópia da evidência (Brasil, 2013). Por este motivo, é preciso analisar qual a melhor técnica a ser empregada, isto é, se as evidências serão coletadas, ou se passarão diretamente à etapa da aquisição/cópia. Para tomar esta decisão, devem ser considerados vários fatores, tais como a volatilidade da evidência, tempo, custo, recursos técnicos e de pessoal, criticidade do sistema, existência de criptografia e até mesmo exigências legais, se houver (Brasil, 2013).

Em relação à volatilidade, importante destacar que o vestígio digital é dividido em duas categorias, os voláteis e não voláteis. O que diferencia um do outro é que o primeiro pode ser facilmente perdido ou adulterado, caso não sejam tomados os devidos cuidados para sua proteção (Brasil, 2013). Assim, é comum que as evidências voláteis sejam diretamente adquiridas (copiadas), não realizando-se a etapa da coleta, a fim de evitar perdas. A exemplo disso, destaca-se a memória RAM e a memória ROM, a primeira é considerada volátil, já que o desligamento do dispositivo ocasiona a perda de todos os dados que não foram guardados de forma permanente. Por outro lado, a memória ROM caracteriza-se pela não volatilidade, já que não há perdas com o seu desligamento (Oliveira, 2019).

Assim, para saber se a etapa da coleta será realizada, bem como quais os procedimentos a serem tomados, primeiramente é necessário saber se a evidência digital está armazenada em dispositivo físico ou encontra-se diretamente na rede. Além disso, é preciso também saber se o dispositivo se encontra ligado ou desligado.

Tratando-se de evidências armazenadas em dispositivo físico não conectado à rede, que se encontre ligado, deve seguir o seguinte procedimento: i) verificar se o vestígio é volátil ou não volátil. Se volátil, segue diretamente para a etapa da aquisição/cópia, a qual será analisada posteriormente. Caso não seja volátil, o próximo

passo é verificar se o dispositivo está estável ou não; ii) se estável, o sistema pode ser desligado normalmente, devendo primeiro desconectar a extremidade ligada ao dispositivo, e não aquela ligada à tomada. Por outro lado, caso instável, o desligamento deve ocorrer por meio da remoção da fonte de alimentação direta do dispositivo ou bateria, ou ambas; iii) em seguida, todos os cabos e portas do dispositivo devem ser etiquetados e protegidos, inclusive, o interruptor de energia, que deve ser isolado com fita; iv) por fim, havendo outras mídias conectadas ao dispositivo, o seu procedimento de coleta dependerá das suas características próprias (Brasil, 2013).

Ainda, há alguns procedimentos específicos, como é o caso do computador portátil. Caso haja alguma evidência volátil, ela deve ser adquirida antes do desligamento do computador portátil, além disso, este deve ser deligado com a retirada da bateria ao invés de pressionar o botão de desligamento, tendo em vista que esta última opção pode ocasionar a alteração ou exclusão de evidencias (Brasil, 2013).

Por outro lado, havendo evidências armazenadas em dispositivo físico não conectado à rede, que se encontre desligado, deve seguir o seguinte procedimento: i) verificar se o dado é volátil ou não. Sendo volátil, é preciso primeiro remover a fonte de energia e bateria e, em seguida, remover e etiquetar a unidade de disco rígido. Caso não seja volátil, é preciso remover as fontes de alimentação diretamente do dispositivo; ii) desconectar os cabos de energia, devendo primeiro desconectar a extremidade ligada ao dispositivo, e não ligada à tomada; iii) proteger os cabos, portas (USB, HDMI, entre outros), entrada de disquete e bandeja, utilizando-se de fita para evitar que fiquem abertos; iv) isolar o interruptor de energia com fita, a fim de evitar a alteração de estado; v) por fim, caso haja alguma mídia adicional conectada no dispositivo, deve-se manuseá-la de acordo com as suas diretrizes específicas; vi) caso haja mídias de armazenamento, como CD e *pen drive*, é recomendado não desconectar do dispositivo (Brasil, 2013).

Por fim, em relação aos dados armazenados em dispositivo conectados à rede ou localizados tão somente na rede, a coleta é mais complexa, vez que há maior risco de perda ou adulteração dos dados, afinal, não se encontram apenas em um local físico, mas sim navegando na rede, gerando risco de alteração por outras pessoas e em outros locais. No entanto, apesar desta dificuldade, a Norma Técnica também prevê alguns procedimentos a serem seguidos para evitar perdas e contaminações: i) traçar as conexões até os dispositivos ligados à rede, a fim de possibilitar a sua reconstrução em momento futuro; ii) certificar-se de que a desconexão da rede

não ocasionará perdas de evidencias digitais; iii) desconectar os dispositivos da rede; iv) isolar os dispositivos desconectados, incluindo cabos e portas; v) em relação aos dispositivos móveis, devem ser selados e etiquetados para evitar operações acidentais de chaves ou botões, além disso, podem ser utilizadas as caixas de *Faraday,* a fim de evitar interferências externas (Brasil, 2013).

Após estas diligências, havendo dispositivo físico, este deverá ser transportado até o local em que posteriormente realizar-se-á sua cópia e perícia. Para o transporte, é preciso que os dispositivos estejam todos acondicionados, a fim de evitar danificações durante o transcurso, devendo-se assegurar o nível de umidade e de transpiração, a temperatura adequada, bem como evitar trajetos prolongados e exposição a radiações ultravioletas ou descargas eletrostáticas. Além disso, caso a pessoa que realizou a coleta não acompanhe o transporte dos dispositivos, recomenda-se realizar a criptografia dos materiais (Machado, 2022).

Em seguida, passa-se a etapa da cópia. Tanto Marshall (2008), quanto a ABNT NBR ISO/IEC 27037 (2013), preveem esta etapa, contudo, trazem uma nomenclatura diferente. Para Marshall (2008), a etapa é denominada exame, a qual consiste em separar e identificar as evidências coletadas que possuem relevância para o caso investigado e, posteriormente, produzir a *image*, isto é, fazer a cópia destas fontes probatórias. Por outro lado, a ABNT NBR ISO/IEC 27037 (2013), nomeia esta etapa como aquisição, consistente na cópia das evidências digitais coletadas e a documentação dos métodos e ferramentas utilizados.

A realização desta etapa tem a função de minimizar os riscos de adulteração ou perda das evidências digitais coletadas, uma vez que a partir deste momento, o manuseio e a perícia recairão sobre a cópia e não sobre o vestígio digital originário, ficando este armazenado, a fim de manter sua integridade (Mendes, 2018). Inclusive, o Procedimento Operacional Padrão n.º 3.1, referente a Perícia Criminal de Informática Forense do Ministério da Justiça, o qual tem a função de orientar os peritos na realização das periciais de dados armazenados em computadores, estabelece a necessidade de duplicação das evidências digitais, justamente para manter os dados originais protegidos de contaminações (Brasil, 2013).

Nesta etapa, a ABNT também traz procedimentos diferentes, a depender se a evidência está armazenada em dispositivo conectado ou desconectado da internet, bem como se está ligado ou deligado. Nos casos em que é possível realizar a coleta do dispositivo, este estará sempre desligado e desconectado da rede, afinal, como já

visto, um dos procedimentos exigidos para realizar a coleta é justamente o desligamento do dispositivo e a desconexão da internet, a fim de que seja transportado para outro local de forma segura (Brasil, 2013).

Diante disso, caso a evidência digital esteja armazenada em um dispositivo físico que se encontre desconectado da rede e desligado, primeiramente é preciso assegurar se realmente está desligado. Após, deve-se remover o armazenamento do dispositivo, local onde ficam guardados os dados digitais, tais como a memória RAM e ROM de um computador. Em seguida, deve-se rotular este armazenamento, documentando a fabricação, nome, modelo, número de série, tamanho e outras informações que entender relevante. Por fim, deve ser realizada a cópia do disco de armazenamento (Brasil, 2013).

Em relação à produção da cópia, a ABNT NBR ISO/IEC 27037 (2013) não traz qual o mecanismo a ser utilizado. Por outro lado, Marshall (2008) estabelece que o dispositivo deve ser conectado a uma estação de processamento e geração de imagem, ou seja, um software de imagem, responsável por ler os dados e passá-los para um arquivo ou um dispositivo separado. Ademais, deve ser utilizado conjuntamente um bloqueador de gravações, o qual trata-se de um sistema informático para impedir a adulteração dos dados durante a cópia (Ramalho, 2017).

Além disso, importante destacar que tanto Marshall (2008) quanto a ABNT NBR ISO/IEC 27037 (2013), preveem a necessidade da criação de duas cópias, a mestra e a de trabalho. A cópia-mestra deverá ficar guardada, podendo ser utilizada somente para criação de outra cópia de trabalho, caso esta se danifique. Já quanto a cópia de trabalho, será utilizada para realização das perícias. Diante disso, nota-se que a produção de duas cópias permite que uma delas fique armazenada e protegida de qualquer adulteração ou perda, uma vez que só a de trabalho será manuseada.

Já nos casos em que há evidências digitais armazenadas em dispositivos ligados, estando ou não conectados à rede, a aquisição/cópia deve ser realizada ao vivo, isto é, no próprio local em que foi encontrado. Isso acontece quando, por alguma impossibilidade, como é o caso das evidências voláteis, o desligamento ou desconexão da rede pode gerar a sua perda ou adulteração, assim, não será possível fazer a sua coleta, ou seja, desligar e desconectar o dispositivo, transportando-o para outro local (Brasil, 2013). A realização da cópia será feita por meio de transferências dos dados do dispositivo físico investigado, para um dispositivo de armazenamento ex-

terno, tais como o disco rígido USB, o qual deverá ser selado, identificado e documentado. Ademais, nestes casos é possível realizar a cópia de forma *online*, contudo, este método pode gerar risco de contaminação (Mendes, 2018).

Após a produção da cópia, é necessário armazená-las em um local seguro, para que sejam preservadas até o fim da cadeia de custódia, ou seja, até que não sejam mais necessárias e possam ser descartadas, motivo pelo qual, a próxima etapa a ser realizada é a do arquivamento e preservação.

Esta etapa consiste em arquivar as cópias em um local seguro, a fim de que permaneçam iguais às evidências digitais originárias durante toda a cadeia de custódia, ou seja, até o momento que possam ser descartadas (Brasil, 2013). Esta etapa busca evitar alterações, mantendo a integridade e autenticidade da evidência digital copiada (Mendes, 2018). No entanto, não há como garantir completamente a autenticidade da prova digital, mas sim, torná-la mais confiável, haja vista a facilidade de fraude e fluidez de seu conteúdo (Santos; Borges; Rodrigues, 2021).

A ABNT NBR ISO/IEC 27037 (2013), estabelece que, caso os dados sejam voláteis, será necessário armazená-los antes em um receptáculo de arquivo lógico, tais como um arquivo em ZIP, e após, este deve ser arquivado em uma mídia de armazenamento digital. Por outro lado, caso o dado não seja volátil, basta que sejam armazenados diretamente na mídia de armazenamento digital[14]. Além disso, a referida norma prevê a necessidade de manter esterilizada esta mídia, isto é, formatada, sem quaisquer outros dados armazenados nela (Brasil, 2013).

Em seguida, após devidamente arquivada, a ABNT NBR ISO/IEC 27037 (2013) estabelece a necessidade de usar uma função de verificação, para comprovar que as cópias ali armazenadas, são iguais às evidências digitais originais (Brasil, 2013). A ferramenta de verificação mais destacada pela norma técnica e pela doutrina, é a utilização do código *hash*.

Para Souza, Munhoz e Carvalho (2023), o código *hash* trata-se de um algoritmo com a função de gerar uma impressão digital do arquivo, ou seja, a partir do seu conteúdo, é criado um código alfanumérico único, que distingue o arquivo de todos os demais, vez que somente ele terá este código. Deste modo, o *hash* possibilita verificar a mesmidade das cópias, isto é, saber se sofreram ou não alteração, isso porque, por

[14] “Dispositivo no qual dados digitais podem ser arquivados” (Brasil, 2013, p. 3).

ser o código produzido a partir do conteúdo do arquivo, cada vez que houver a alteração dele, mesmo que seja de um único *bit*, gerará outro código *hash* diferente (Ramalho, 2017).

Logo, o *hash* garante a autenticidade e integridade da prova, visto que será possível saber quando houve a alteração das evidências digitais armazenadas. Assim, caso não haja registro da alteração realizada, ter-se-á a presunção de uma violação indevida no documento, o que, por óbvio, permitirá que a prova seja objeto de questionamento futuro.

A próxima etapa é a perícia. Contudo, a NBR ISO/IEC 27037 (2013) não traz menção a esta etapa, já que, conforme ela própria prevê, somente fornece diretrizes sobre o manuseio inicial da evidência digital. Por outro lado, Marshall (2008) estabelece que a próxima etapa a ser realizada é a análise, isto é, a perícia da evidência digital coletada, no entanto, nada prevê sobre como esta deve ocorrer.

Os autores Souza, Munhoz e Carvalho (2023), também trazem a etapa da perícia, entendendo que apesar das evidências digitais terem seguido o procedimento correto, ainda há necessidade da realização desta etapa, a fim de que seja possível verificar em juízo se realmente a prova se mantêm íntegra e autêntica. Este entendimento está muito ligado com o princípio da desconfiança, anteriormente discutido, isso porque, as evidências não podem ser pré-estabelecidas como autênticas, devendo-se sempre submetê-las a um processo de acreditação (Prado, 2019). Assim, a realização da perícia torna-se cada vez mais necessária, a exemplo disso, destaca-se a evolução da inteligência artificial, como é o caso do sistema *deepfakes*, capaz de criar vídeos falsos, colocando o rosto e a voz de uma pessoa, sem isso nunca ter existido (Souza; Munhoz; Carvalo, 2023).

Quanto a forma da realização da perícia, primeiramente, Carvalho (2020) destaca que esta deve recair sobre a cópia da evidência digital:

> a evidência digital original deve ser mantida em segurança e devidamente documentada no formulário de cadeia de custódia, respeitando sua integridade. Todo e qualquer procedimento para averiguação e análise da evidência deve ser feito com uma cópia forense, ou a cópia da cópia forense. Desta forma, conseguimos preservar o material original, e trabalhar com as cópias para fins elucidativos (Carvalho, 2020, p. 134-138).

Além disso, Souza, Munhoz e Carvalho (2023) estabelecem três etapas a serem seguidas na realização da perícia. A primeira delas é o exame, consistente em

verificar o material coletado, a fim de identificar quais são os dados digitais relevantes para serem periciados. A segunda etapa é a análise, por meio da qual o perito transforma estes dados em informação, ou seja, busca reconstruir todos os passos seguidos pelo investigador, desde o momento do isolamento e identificação do vestígio, até sua coleta, cópia e arquivamento. Por fim, a terceira etapa é a confecção do laudo, no qual o perito fará toda a documentação das etapas da perícia e apresentará as descobertas e resultados obtidos, devendo ser fundamentado com rigor técnico, utilizando-se de livros, manuais, artigos científicos e normas técnicas.

Ainda, o Brasil prevê a norma técnica intitulada como Procedimento Operacional Padrão de Perícia Criminal, do Ministério da Justiça, o qual estabelece diretrizes quanto a informática forense em relação aos exames periciais de: mídia de armazenamento computacional; equipamento computacional portátil; local de informática e local de internet (Brasil, 2013).

Por fim, em relação ao perito, utilizando-se analogicamente da cadeia de custódia prevista no Código de Processo Penal, o profissional deve ser um perito oficial, isto é, o servidor público que trabalha em um órgão público de segurança, responsável por realizar perícias técnicas e científicas, buscando provas que podem ajudar na solução da infração penal investigada (Souza; Munhoz; Carvalho, 2023).

A próxima etapa é a documentação. Em relação a ela, a ABNT ISO/IEC 27037 (2013) não a prevê como uma etapa propriamente dita, mas estabelece a necessidade de sua realização. Para a norma, a cadeia de custódia é justamente a documentação cronológica de todo o manuseio da evidência digital, ou seja, todas as atividades realizadas durante a identificação, coleta, aquisição e preservação das evidências, bem como quais foram os responsáveis pela realização destas etapas.

Já para Marshall (2008), esta etapa é chamada de relatório, responsável pela descrição de todos os procedimentos realizados. Ademais, estabelece que deverá ser aplicada uma linguagem de fácil entendimento, já que quem analisará estes documentos serão pessoas da área do direito, tais como juízes, promotores e defensores, os quais não possuem conhecimento específico na área da TI. Além disso, os procedimentos devem ser descritos de forma minuciosa, justamente para que as pessoas atuantes no processo conheçam exatamente toda a cadeia de custódia percorrida, sem qualquer lacuna (Mendes, 2018).

Ainda, Souza (2021), destaca que não deve ser documentado apenas o procedimento realizado e os responsáveis, mas sim todas as informações relacionadas

às evidências digitais, tais como a documentação do código *hash*, o local onde estão armazenadas, os momentos e os motivos em que estas evidências são acessadas e quem realizou este acesso.

Diante disso, nota-se que a documentação não se trata da última etapa, mas sim aquela que deve ser realizada durante toda a cadeia de custódia, do início ao fim, devendo ser levada ao processo junto com as evidências digitais e com a perícias realizadas, a fim de que as partes e o juiz possam verificar se a prova é realmente autêntica e Íntegra, ou se, por algum motivo, sofreu perdas ou adulterações. Logo, verifica-se que a documentação é imprescindível para averiguar se a cadeia de custódia foi cumprida.

Finalmente, a última etapa é a destruição dos vestígios. Para Mendes (2018), a etapa final da cadeia de custódia da prova digital é o arquivamento do material ou a destruição das provas irrelevantes. Diante disso, nota-se que após a utilização da evidência digital no processo, esta deverá retornar para o arquivamento, etapa já vista anteriormente, até o momento da sua destruição. Contudo, não há previsão na ABNT ISO/IEC 27037 (2013), nem mesmo nas doutrinas mencionadas, de quando as evidências digitais devem ser destruídas, ou seja, em que momento elas se tornarão irrelevantes e não precisão mais ser guardadas.

4.3.2 Os impasses para o cumprimento da cadeia de custódias da prova digital

O primeiro impasse relacionado a tal temática é a carência de lei específica, não só quanto as etapas da cadeia de custódia da prova digital, mas também a previsão de quando ocorre a quebra e quais suas consequências. É sabido que a Lei 13.964/2019 instituiu no Código de Processo Penal a cadeia de custódia de provas. Todavia, as mudanças implementadas nada falam sobre a cadeia de custódia das provas digitais, sendo que, “não há, até o momento, na legislação brasileira, uma tratação específica relativa aos procedimentos que devem ser adotados para este particular tipo de provas” (Parodi, 2022, não paginado). Portanto, atualmente o que há são normas gerais sobre a cadeia de custódia de provas, aplicáveis somente aos vestígios materiais.

A única normatização referente a cadeia de custódia da prova digital, trata-se da norma técnica ABNT/ISO 27037 de 2013. Contudo, embora a ABNT seja um órgão de normatização técnica reconhecida oficialmente pelo Brasil, a sua norma 27037 não

é cogente, uma vez que não há lei que expressamente a reconheça como tal, inclusive, sua própria redação indica que são apenas recomendações (Parodi, 2020). Também, importante ressaltar que a norma não é completa, tendo em vista que prevê apenas algumas etapas iniciais da cadeia de custódia (Almas, 2021).

Ademais, não se pode perder de vista que a norma ABNT/ISSO 27037 é do ano de 2013, ou seja, suas previsões podem não mais satisfazer as necessidades de custódia das atuais provas digitais, ante o avanço tecnológico. Aliás, a questão da mutabilidade das relações informáticas acaba por recomendar que o tema da cadeia de custódia das provas digitais seja regulado por lei específica ou norma técnica oficial, considerando que, com o surgimento de novas necessidades, aquelas podem ser alteradas/adaptadas mais rápida e facilmente:

> De fato, definir em lei procedimentos técnicos relativos à cadeia de custódia de evidências digitais poderia ser inútil ou até contraproducente, pois, num ambiente de rápida e constante evolução tecnológica, haveria grande chance de tais procedimentos ficarem rapidamente ultrapassados e não mais conformes às melhores práticas. Por essa razão, é certamente melhor criar uma lei, como aquela em foco, que defina conceitos e critérios de cunho geral, remetendo a normas técnicas de mais fácil atualização, a definição detalhada dos procedimentos relativos a âmbitos em constante evolução, como o mundo digital. (Parodi, 2020, não paginado).

Diante disso, a ausência de lei específica sobre o assunto traz enorme insegurança jurídica, em virtude da impossibilidade de se decidir qual a consequência da quebra da cadeia de custódia da prova digital, e pior, quando esta quebra se configura, delegando para o Poder Judiciário a responsabilidade de debruçar-se sobre o tema, acarretando em decisões conflitantes:

> A ausência de disciplina legal sobre provas digitais já demonstra, por si, a séria insuficiência no trato da temática no Brasil. A despeito de todo o avanço tecnológico, muito pouco se evoluiu no país na disciplina das provas digitais e dos meios de obtenção de prova relacionados à tecnologia e à internet. As poucas normas existentes são insuficientes para lidar com a complexidade das questões que surgem em tordo do crescente uso da tecnologia na produção de provas. Este estado de anomia vem sendo preenchido por decisões judiciais contraditórias e pequena parcela de casos chegam a ser tratados em instâncias superiores (Oliveira, 2023, não paginado).

Logo, a ausência de regulamentação específica sobre a cadeia de custódia das provas digitais trata-se de grave lacuna legislativa, que coloca em risco toda a legalidade das provas digitais e do próprio processo penal brasileiro, ainda marcado

com traços do sistema inquisitório, já que, a depender do julgador, eventual quebra poderá ser tratada como mera irregularidade.

Diante disso, nota-se que a regulamentação sobre esta matéria é de suma importância, isso porque, caso haja previsão das etapas, de quando ocorre a quebra e das suas consequências, os profissionais que atuam durante a persecução penal serão obrigados a seguir tudo o que está nesta lei, justamente por ela ter força impositiva. Além disso, o Poder Judiciário saberá quando não houve o cumprimento integral da cadeia de custódia e também saberá qual a atitude a ser tomada, evitando desta forma, decisões contraditórias e, consequentemente, inseguranças jurídicas.

Ainda, outro impasse quanto a este instituto, é a falta de previsão quanto as consequências da quebra da cadeia de custódia da prova penal digital. A própria doutrina não possui consenso, havendo duas correntes. Para a primeira corrente, da qual é adepto Lopes Júnior, a consequência “deve ser a proibição de valoração probatória com a consequente exclusão física dela e de toda a derivada”, ou seja, o autor entende que a prova é ilícita (Lopes Júnior, 2020, p. 414). Já a segunda corrente defende que a consequência da quebra será a atribuição de menor valor ao meio de prova. Para Gustavo Badaró “as irregularidades da cadeia de custódia não são aptas a causar a ilicitude da prova, devendo o problema ser resolvido, com redobrado cuidado e muito maior esforço argumentativo, no momento da valoração” (Badaró, 2017, p. 533).

O Superior Tribunal de Justiça, atualmente, vem entendendo que a quebra da cadeia de custódia da prova penal digital acarretará na ilicitude desta, ou seja, deverá ser desentranhada dos autos. É o que se verifica do julgado AgRg no RHC 143.169 do STJ, que se tornou precedente deste Tribunal. Na referida decisão, após a coleta de vestígios digitais por policiais, sem qualquer documentação do procedimento adotado, nem mesmo a criação do código *hash*, o Tribunal entendeu haver a quebra da cadeia de custódia, uma vez que, com a falta destes procedimentos, tornou-se impossível saber se os vestígios localizados no mundo real, eram os mesmos inseridos no processo (Brasil, 2023).

Assim, por meio deste julgado, pode-se concluir dois pontos importantes. O primeiro deles é que, apesar de não haver previsão quanto as etapas da cadeia de custódia da prova digital, o STJ vem entendendo que se faz necessário, ao menos, a documentação do procedimento adotado por quem fez a coleta dos vestígios, inclusive protegendo-os por meio da utilização do código *hash*, justamente para que durante o processo, as partes consigam averiguar se houve alguma alteração ou perda

da prova. Além disso, outro ponto, é que o STJ passou a entender que, a quebra da cadeia de custódia da prova digital, impossibilita averiguar a mesmidade da prova, logo, esta deve ser desentranhada dos autos, inclusive em sede de habeas corpus, adotando-se assim, a teoria da ilicitude (Brasil, 2023).

Por fim, outro impasse é a falta de estrutura das instituições e dos profissionais que atuam durante a persecução penal, tais como a polícia, Ministério Público, Judiciário, Defensoria Pública e advogados. Como verifica-se da jurisprudência supramencionada, a prova foi desentranhada dos autos justamente porque os policiais não realizaram a documentação do procedimento e a utilização do código *hash*, contudo, isso acontece, na maioria das vezes, não pela má-fé destes, mas sim pela falta de conhecimento técnico e treinamento. Assim, não se pode ignorar que a falta de recursos, de pessoal e de capacitação é um grande empecilho para a cadeia de custódia de todos os tipos de prova, principalmente a da prova digital:

> Comumente alguns aspectos relacionados à cadeia de custódia são despercebidos ou descumpridos pelos profissionais de segurança pública envolvidos, seja pelo desinteresse ou desconhecimento sobre o assunto. Os policiais responsáveis pelo isolamento e preservação do local de crime (first responders) desempenham um papel de extrema importância na cena do crime, porém muitas vezes desconhecem procedimentos básicos para evitar que vestígios materiais sejam perdidos, destruídos ou mesmo contaminados. Oferecer treinamento adequado para capacitar esses profissionais é fundamental (Machado, 2017, p. 10).

Tal situação é preocupante, considerando a volatilidade deste tipo de prova, cuja manipulação, além de específica, deve ser integralmente documentada. Certamente, a total observância da cadeia de custódia no Brasil estará inteiramente relacionada com o treinamento dos agentes responsáveis pela coleta da evidência digital e com a aquisição de recursos técnicos e científicos, ou seja, o poder público deverá investir recursos para que a cadeia de custódia não passe de mera previsão legal.

Em suma, a criação de lei específica sobre a cadeia de custódia da prova digital é essencial para delimitar as etapas integrantes da cadeia de custódia, assim como as peculiaridades a serem observadas em cada etapa, da coleta até a destruição. Somente assim haverá certeza quanto a adoção do correto procedimento em cada caso concreto. Ainda, a norma que regulamentar a matéria também deverá trazer as consequências de sua quebra, evitando que o julgador esteja livre para decidir se a inobservância do procedimento será tida como mera irregularidade ou acarretará

na ilicitude da prova. Todavia, de nada adiantará previsão legal, se os sujeitos envolvidos na custódia da prova digital não possuírem capacitação técnica para garantir sua integral observância, logo, faz-se necessário também, investimento e treinamento destes profissionais.

5 CONLCUSÃO

Por meio da pesquisa sobre a cadeia de custódia da prova digital, foi possível constatar a relevância de tal temática, devido à ampla utilização de meios eletrônicos e virtuais nas mais diversas áreas e no próprio cotidiano das pessoas, resultando, por consequência, na massiva criação e armazenamentos de dados digitais. Assim, considerando a importância que a prova detém no processo penal, mostra-se imprescindível conhecer quais são as etapas da cadeia de custódia da prova digital, inclusive, as consequências de sua quebra, e os desafios a serem combatidos para garantir sua preservação.

Tal objetivo geral foi alcançado, uma vez que, por meio de uma análise jurisprudencial, doutrinária, e da ABNT NBR ISO/IEC 27037 2013, foi possível construir possíveis etapas da cadeia de custódia da prova digital. Além disso, por meio da doutrina e da jurisprudência, também foi possível verificar quais as possíveis consequências da quebra da cadeia de custódia desta espécie de prova, bem como saber quais os impasses existentes para o respeito e preservação deste instituto.

Para tanto, por meio do primeiro capítulo, constatou-se que hoje vivemos na quarta revolução industrial e na chamada sociedade da informação, caracterizadas pelo avanço tecnológico dos dispositivos eletrônicos e da internet. Graças a isso, por ser o direito reflexo da sociedade, a área criminal sofreu influências, seja na prática de cibercrimes, na utilização do meio digital para as investigações, e até mesmo o surgimento de uma nova espécie de prova, qual seja, a prova digital.

Em seguida, no segundo capítulo, atingiu-se o segundo objetivo específico do trabalho, qual seja, entender os principais aspectos da prova penal digital. Inicialmente, constatou-se que a prova é um importante instrumento para concretização do devido processo legal, sendo imprescindível na busca da melhor decisão. Após, verificou-se que a prova digital se refere a informações e dados produzidos e/ou armazenados digitalmente, utilizados para confirmar ou rejeitar determinado fato no processo. Ainda, suas características são distintas das demais provas, vez que são imateriais, voláteis e suscetíveis de clonagem, alteração e perda. Por fim, quanto aos meios de obtenção da prova digital, constatou-se que existem duas formas, a primeira por meio da busca e apreensão de dispositivos eletrônicos, e a segunda por meio da interceptação remota de dados, sendo que a forma de produção, ou seja, de inserção no processo penal, deve ocorrer por meio da perícia de tais evidencias digitais.

Finalmente, no terceiro capítulo, descobriu-se quais são as possíveis etapas da cadeia de custódia da prova digital e os impasses a serem combatidos e solucionados para sua preservação, atingindo-se assim, o terceiro objetivo específico e a resposta do problema da presente pesquisa. Por meio de uma construção doutrinária e jurisprudencial, constatou-se que existem nove etapas da cadeia de custódia da prova digital, quais sejam, isolamento, identificação, coleta, transporte, cópia/aquisição, arquivamento/preservação, perícia/análise, documentação/relatório e destruição.

Além disso, constatou-se três principais empecilhos a serem combatidos, para o cumprimento deste instituto, sendo eles, a falta de legislação específica sobre as etapas da cadeia de custódia da prova digital, a falta de previsão quanto aos efeitos da quebra da cadeia e, por fim, a falta de investimento das instituições e de treinamento técnico dos profissionais atuantes na persecução penal.

Diante disso, verifica-se que a hipótese do trabalho foi confirmada, já que inexiste lei específica que regulamente o tema da presente pesquisa, existindo apenas uma norma técnica, a ABNT NBR ISO/IEC 27037, a qual além de ser incompleta e ultrapassada, sequer possui força cogente. Além disso, constatou-se que não basta a criação de lei, sendo necessário também investimento e capacitação técnica dos órgãos e dos profissionais, principalmente dos policiais, tendo em vista que estes, geralmente, são os primeiros a terem acesso aos vestígios digitais de uma infração penal.

Por fim, importante destacar que a pesquisa sobre tal temática pode ainda ser aprofundada em outros trabalhos, uma vez que existem diversas formas de produção de dados digitais, podendo, a cadeia de custódia, varear em cada um desses casos específicos, como por exemplo, a cadeia de custódia de um celular, de uma interceptação telefônica e até mesmo das redes sociais.

REFERÊNCIAS

ALMAS, Amanda Costa das. A aplicabilidade da cadeia de custódia em dados digitais utilizados como prova no processo penal brasileiro. **IBCCRIM - Laboratório de Ciências Criminais,** Porto Alegre/RS, 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ibccrim.org.br/app/webroot/media/documentos/doc-07-10-2021-11-44-50-262499.pdf. Acesso em: 05 set. 2023.

ARANHA, Adalberto José Queiroz. Telles. de Camargo. **Da prova no processo penal**. 7ª ed. São Paulo/SP: Saraiva, 2008.

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

ASSUMPÇÃO, T. A. A.; GARCIA, M. V. R.; LOPES, C. L. R. As revoluções industriais e o surgimento do proletariado urbano. **Brasil Para Todos – Revista Internacional**: **Anais do VIII Seminário Internacional de Integração Étnico-Racial**, Guarulhos/SP, v. 8, n. 1, p. 22 a 26, out. de 2020. Disponível em: https://ojs.eniac.com.br/index.php/Anais_Sem_Int_Etn_Racial/article/view/646/pdf. Acesso em: 26 dez. 2022.

AVENA, Norberto. **Processo Penal**. 14ª e.d. Rio de Janeiro/RJ: Grupo GEN, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559645084/. Acesso em: 28 mar. 2023.

BADARÓ, Caio; MATIDA, Janaina. Exame da cadeia de custódia é prejudicial a todas as decisões sobre fatos. **Consultor Jurídico**, 13 ago. 2021. Disponível em: https://www.conjur.com.br/2021-ago-13/limite-penal-exame-cadeia-custodia-prejudicial-todas-decisoes-fatos. Acesso em: 06 jul. 2023.

BADARÓ, Gustavo Henrique Righi Ivahy. A cadeia de custódia e sua relevância para a prova penal. In: SIDI, Ricardo; LOPES, Bezerra Anderson (Org). **Temas atuais da investigação preliminar no processo penal.** Belo Horizonte: Editora D'Plácido, 2017. Disponível em: https://www.academia.edu/41762446/A_cadeia_de_cust%C3%B3dia_e_sua_relev%C3%A2ncia_para_a_prova_penal. Acesso em: 04 jul. 2023.

BADARÓ, Gustavo Henrique Righi Ivahy. **Ônus da prova no processo penal**. São Paulo: RT, 2003.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção probatória na prova digital e a importância da cadeia de custódia. **Instituto Brasileiro de Ciências Criminais,** São Paulo/SP, v. especial, n. especial, p. 7-10, mai. 2021. Disponível em: https://www.badaroadvogados.com.br/artigos-2021-os-standards-metodologicos-de-producao-da-prova-na-prova-digital-e-a-importancia-da-cadeia-de-custodia-gustavo-badaro-ibccrim-junho-2021.html. Acesso em: 24 fev. 2023.

BADARÓ, Gustavo Henrique Righi Ivahy. **Processo Penal**. 6ª e.d. São Paulo: Thomson Reuters Brasil, 2018.

BAUTISTA, Juan Carlos Urazán. **La cadena de custodia en el nuevo codigo de procedimento penal.** Faceta Juridica. Bogotá: Leyer, 2005. Disponível em: <https://fundacionluxmundi.com/custodia.php>. Acesso em: 05 jul. 2023.

BONIATI, Bruno Batista; PREUSS, Evandro; FRANCISCATTO, Roberto. **Introdução à Informática**. Frederico Westphalen/RS: Universidade Federal de Santa Maria, Colégio Agrícola de Frederico Westphalen, 2014. Disponível em: http://heleno.info/ensino/livro.pdf. Acesso em: 04 jan. 2023.

BRASIL. **Constituição Federal (1988).** Diário Oficial da União, Brasília/DF: palácio do planalto, 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 mar. 2023.

BRASIL. **Decreto-Lei 3.689, de 03 de outubro de 1941**. Código de Processo Penal. Diário Oficial da União, Brasília/DF: palácio do planalto, 03 out. 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 05 mar. 2023.

BRASIL é 5º maior alvo de cibercrimes. **Globo Comunicações e Participações - Negócios**, 12 set. 2021. Disponível em: https://revistapegn.globo.com/Tecnologia/noticia/2021/09/pegn-brasil-e-5o-maior-alvo-de-cibercrimes.html. Acesso em: 03 jan. 2023.

BRASIL. **Lei 9.296/96, 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal - Interceptação telefônica e telemática. Diário Oficial da União, Brasília/DF: palácio do planalto, 24 JUN. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 23 mar. 2023.

BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília/DF: palácio do planalto, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 set. 2023.

BRASIL. **Lei n. º 13.441, de 08 de maio de 2017**. Alterou a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Diário Oficial da União, Brasília-DF: palácio do Planalto, 08 maio 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm. Acesso em: 12 jan. 2023.

BRASIL. **Lei 13.964, de 24 de dezembro de 2019**. Aperfeiçoou a legislação penal e processual penal – conhecida como Lei Anticrime. Diário Oficial da União, Brasília/DF: palácio do planalto, 24 dez. 2019. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 07 mar. 2023.

BRASIL. Ministério da Justiça. **Procedimento Operacional Padrão Perícia Criminal**. Brasília, DF: Ministério da Justiça, 2013. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf. Acesso em: 01 set. 2023.

BRASIL. **Portaria Senasp nº 82, de 16 de julho de 2014**. Estabelece as Diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígios. Brasília/DF: Diário Oficial da União (nº 136, Seção 1, pág. 42), 16 jul. 2014. Disponível em: https://diariofiscal.com.br/ZpNbw3dk20XgIKXVGacL5NS8haIoH5PqbJKZaawfaDwCm/legislacaofederal/portaria/2014/senasp82.htm. Acesso em: 01 ago. 2023.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 143.169 – RJ.** Penal e processual penal. Agravo regimental no recurso ordinário em habeas corpus. operação open doors. Furto, organização criminosa e lavagem de dinheiro. Acesso a documentos de colaboração premiada. Falha na instrução do habeas corpus. Cadeia de custódia. Inobservância dos procedimentos técnicos necessários a garantir a integridade das fontes de prova arrecadadas pela polícia. Falta de documentação dos atos realizados no tratamento da prova. Confiabilidade comprometida. provas inadmissíveis, em consequência. Agravo regimental parcialmente provido para prover também em parte o recurso ordinário [...]. Plenário. Agravante: R L S M. Agravado: Ministério Público do Estado do Rio de Janeiro. Relator: Min. Jesuíno Rissato e Min. Ribeiro Dantas, 07 fev. 2023. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.conjur.com.br/dl/stj-reconhece-quebra-cadeia-custodia.pdf. Acesso em: 20 ago. 2023.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus nº 160.662/RJ.** Penal e processual penal. Habeas corpus substitutivo de recurso ordinário. Utilização do remédio constitucional como sucedâneo de recurso. Não conhecimento do writ. Precedentes do supremo tribunal federal e do superior tribunal de justiça. quebra de sigilo telefônico e telemático autorizada judicialmente. Supressão de instância com relação a um dos pacientes. Presença de indícios razoáveis da prática delituosa. Indispensabilidade do monitoramento demonstrada pelo modus operandi dos delitos. crimes punidos com reclusão. Atendimento dos pressupostos do art. 2º, i a iii, da lei 9.296/96. legalidade da medida. Ausência de preservação da integralidade da prova produzida na interceptação telefônica e telemática. Violação aos princípios do contraditório, da ampla defesa e da paridade de armas. Constrangimento ilegal evidenciado. Habeas corpus não conhecido. Ordem concedida, de ofício. Plenário. Impetrante: F U F e outros. Impetrado: Tribunal Regional Federal da 2ª Região. Relatora: Min. Assusete Magalhães, 18 fev. 2014. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1297583&num_registro=201000153608&data=20140317&formato=PDF. Acesso em: 20 set. 2023.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus nº 653.515 – RJ.** Habeas Corpus. Tráfico de drogas e associação para o narcotráfico. Quebra da cadeia de custódia da prova. Ausência de lacre. Fragilidade do material probatório residual. Absolvição que se mostra devida. Associação para o narcotráfico. Higidez na condenação. Ordem concedida. [...]. Requerente: A R S. Requeridos: Ministério Público do Estado do Rio de Janeiro e Ministério Público Federal. Plenário. Impetrado: Tribunal de Justiça do Estado do Rio de Janeiro. Relatora: Min. Laurita Vaz, 26 out. 2023. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.tjmt.jus.br/intranet.arq/cms/grupopaginas/105/1081/Quebra_da_cadeia_de_cust%C3%B3dia_n%C3%A3o_gera_nulidade_obrigat%C3%B3ria_da_prova_define_Sexta_Turma.pdf. Acesso em: 20 ago. 2023.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus nº 762.844 – SP.** Habeas Corpus. Processual penal. Razões do writ dissociadas da motivação da decisão proferida na origem. Ausência de impugnação à conclusão da decisão impugnada. Violação do princípio da dialeticidade. Mandamus não conhecido [...]. Plenário. Impetrante: I S A B e outros. Impetrado: Tribunal de Justiça do Estado de São Paulo. Paciente: B F L F. Relatora: Min. Laurita Vaz, 01 ago. 2023. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=199930895&num_registro=202202485833&data=20230802. Acesso em: 08 set. 2023.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus 51.531/RO.** Penal. processual penal. Recurso ordinário em habeas corpus. Tráfico de drogas. Nulidade da prova. Ausência de autorização judicial para a perícia no celular. Constrangimento ilegal evidenciado. 1. Ilícita é a devassa de dados, bem como das conversas de WhatsApp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial. 2. Recurso ordinário em habeas corpus provido, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos. Plenário. Recorrente: L S S. Recorrido: Ministério Público do Estado de Rondônia: Min. Nefi Cordeiro, 19 abr. 2016. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1497056&num_registro=201402323677&data=20160509&formato=PDF. Acesso em: 10 set. 2023.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 63.562 – ES.** Processual penal, recurso ordinário em habeas corpus, decisão de recebimento da denúncia, fundamentação exaustiva, prescindibilidade, gravação de conversa por um dos interlocutores, prova lícita, recurso desprovido [...]. Plenário. Recorrente: M L DA S. Recorrido: A DE A B N, V S L. Relator: Min. Felix Fischer, 10 dez. 2015. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1467087&tipo=0&nreg=201502150954&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20151210&formato=PDF&salvar=false. Acesso em: 03 abr. 2023.

BRASIL. Superior Tribunal de Justiça**. Recurso em Habeas Corpus nº 99.735 – SC**. Recurso ordinário em habeas corpus. penal e processo penal. tráfico de drogas e associação ao tráfico. autorização judicial de espelhamento, via whatsapp web, das conversas realizadas pelo investigado com terceiros. analogia com o instituto da

interceptação telefônica. impossibilidade. presença de disparidades relevantes. ilegalidade da medida. reconhecimento da nulidade da decisão judicial e dos atos e provas dependentes [...]. Plenário. Recorrente: A C DA C. Recorrido: D C DA C. Relator: Ministra Laurita Vaz, 27 nov. 2018. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1777437&num_registro=201801533498&data=20181212&peticao_numero=-1&formato=PDF. Acesso em: 03 abr. 2023.

BRASIL. Supremo Tribunal Federal. **Eemb. Decl. no Recurso Extraordinário 625.263 Paraná.** Embargos de declaração no agravo regimental no recurso extraordinário, inexistência dos vícios do art. 619 do código de processo penal, embargos de declaração rejeitados, 1. Não merecem acolhida os Embargos de Declaração quando a decisão recorrida não padece de ambiguidade, obscuridade, contradição ou omissão, 2. Embargos de Declaração rejeitados. Pleno. Embargante: I R T. Embargado: J C C G F. Plenário. Relator: Min. Alexandre de Moraes, 16 ago. 2022. Disponível em: https://portal.stf.jus.br/processos/downloaPeca.asp?id=15352817202&ext=.pdf. Acesso em: 03 abr. 2023.

BRASIL. Supremo Tribunal Federal**. Habeas Corpus 91.867 Pará**. Habeas corpus. nulidades: (1) inépcia da denúncia; (2) ilicitude da prova produzida durante o inquérito policial; violação de registros telefônicos do corréu, executor do crime, sem autorização judicial; (3) ilicitude da prova das interceptações telefônicas de conversas dos acusados com advogados, porquanto essas gravações ofenderiam o disposto no art. 7º, ii, da lei 8.906/96, que garante o sigilo dessas conversas. vícios não caracterizados. Ordem denegada [...]. Segunda Turma. Recorrente: D R S. Recorrido: L R S. Relator: Min. Gilmar Mendes, 24 abr. 2012. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328. Acesso em: 03 abr. 2023.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus 168.052 São Paulo.** Habeas corpus. 2. Acesso a aparelho celular por policiais sem autorização judicial. Verificação de conversas em aplicativo WhatsApp. Sigilo das comunicações e da proteção de dados. Direito fundamental à intimidade e à vida privada. Superação da jurisprudência firmada no HC 91.867/PA. Relevante modificação das circunstâncias fáticas e jurídicas. Mutação constitucional. Necessidade de autorização judicial. 3. Violação ao domicílio do réu após apreensão ilegal do celular. 4. Alegação de fornecimento voluntário do acesso ao aparelho telefônico. 5. Necessidade de se estabelecer garantias para a efetivação do direito à não autoincriminação. 6. Ordem concedida para declarar a ilicitude das provas ilícitas e de todas dela derivadas. Segunda Turma. Paciente: R R L. Impetrante: A M B. Coator: Superior Tribunal de Justiça. Relator: Min. Gilmar Mendes. 9 a 19 out. 2020. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://portal.stf.jus.br/processos/downloadPeca.asp?id=15345143997&ext=.pdf. Acesso em: 12 set. 2023

CARNEIRO, Adenele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico**, Rio Grande/RS, 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 11 jan. 2023.

CARVALHO, Romullo; SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre. **Manual prática de provas digitais**. São Paulo/SP: Revista dos Tribunais, 2023.

CARVALHO, Romullo Wheryko Rodrigues de. A importância da cadeia de custódia na computação forense. **Revista Brasileira de Criminalística**, [S.L], v.9, n. 2, p. 134-138, 8 jul. 2020. Disponível em: https://revista.rbc.org.br/index.php/rbc/article/view/463. Acesso em: 05 set. 2023.

CASEY, Eoghan. **Digital evidence and computer crime**: forensic science, computers, and the Internet. 2ª ed. San Diego/London: Elsevier Academic Press, 2004.

CASTELLS, Manuel. **A sociedade em rede.** Tradução de Roneide Venancio Majer. 6ª ed. São Paulo/SP: Paz e Terra, 2002. Disponível em: https://globalizacaoeintegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf. Acesso em: 29 dez. 2022.

CAVALCANTI, Zedequias Vieira; SILVA, Mauro Luis Siqueira. A importância da Revolução Industrial no
mundo da tecnologia. **VII EPCC, Encontro Nacional de Produção científica,** Maringá/PR, out. 2011. Disponível em: https://rdu.unicesumar.edu.br/bitstream/123456789/6395/1/zedequias_vieira_cavalcante2.pdf. Acesso em: 22 dez. 2022.

COLOMBO, Jamires de Fátima; LUCCA FILHO, João de. Internet das coisas (IOT) e indústria 4.0: revolucionando o mundo dos negócios. **Revista Interface Tecnologica**, São Paulo/SP, v. 15, n. 2, p. 72-85, dez. 2018. Disponível em: https://revista.fatectq.edu.br/index.php/interfacetecnologica/article/view/496. Acesso em: 30 dez. 2022.

CUNHA, Guilherme Bernardino da; MACEDO, Ricardo Tombesi; SILVEIRA, Sidnei Renato. **Informática Base**. Santa Maria/RS: UFSM, NTE, 2017. E-book. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/17138/Curso_Lic-Computa%C3%A7%C3%A3o_Informatica-Basica.pdf?sequence=1&isAllowed=y. Acesso em: 29 dez. 2022.

CUNHA, Murilo Bastos da; CAVALCANTI, Cordélia Robalinho de Oliveira. Dicionário de Biblioteconomia e Arquivologia. Brasília: Briquet de Lemos/ Livros, 2008.p.212.

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

DAMBROS, Gabriel Herrmann. **Revolução tecnológica, redes de interação e cibercrimes:** considerações sobre os desafios e os limites da persecução penal no enfrentamento dos delitos praticados por meio da rede. 2021. Monografia (Bacharelado). Curso de Direito, Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Ijuí/RS, 2021. Disponível em: https://bibliodigital.unijui.edu.br:8443/xmlui/bitstream/handle/123456789/7428/Gabriel%20Herrmann%20Dambros.pdf?sequence=1&isAllowed=y. Acesso em: 02 jan. 2023.

DEAN, Brian. Principais estatísticas do TikTok: dados sobre usuários, crescimento e mais em 2022. **Semrush Blog**, 28 nov. 2022. Disponível em: https://pt.semrush.com/blog/estatisticas-tiktok/. Acesso em: 03 jan. 2023.

DEZEM, Guilherme Madeira. Curso de Processo Penal. 2ª e.d. São Paulo/SP: Revista dos Tribunais, 2016.

DEZEM, Guilherme Madeira; SOUZA, Luciano Anderson de. **Comentários ao pacote anticrime:** Lei 13.964/2019. São Paulo/SP: Thomson Reuters Brasil, 2020.

DIAS, Renata Rampim de Freitas. **Internet das coisas sem mistérios**: uma nova inteligência para os negócios. São Paulo: Netpress Books, 2016.

DUARTE, Daniel Nascimento. “Lei Anticrime” e a nociva restrição legal de aplicabilidade da cadeia de custódia da Prova Penal. **Boletim IBCCRIM**. São Paulo, v. 28, n. 335, 2020. Disponível em: http://ibccrim.vpn.acelerati.com.br:5180/biblioteca/asp/primapdf.asp?codigoMidia=105058&iIndexSrv=1. Acesso em: 28 ago. 2023.

EDUVIRGES, J. R.; SANTOS, M. N. D. A contextualização da internet na sociedade da informação. **Múltiplos Olhares em Ciência da Informação**, v. 3, n. 2, p. 1-13, 2013. Disponível em: https://periodicos.ufmg.br/index.php/moci/article/view/17450/14233. Acesso em: 29 dez. 2022.

FERNANDES, Ana Júlia Feiber. **A Problemática da Utilização da Prova Digital no Processo Penal Brasileiro Diante da Ausência de Regulamentação**. Orientador: Chiavelli Facenda Falavigno. 2019. Trabalho de Conclusão de Curso (Bacharel em Direito). Faculdade de Direito - Universidade Federal de Santa Catarina, Florianópolis/SC: 2019. Disponível em: https://repositorio.ufsc.br/handle/123456789/199471#:~:text=TCC%20Direito-,A%20problem%C3%A1tica%20da%20utiliza%C3%A7%C3%A3o%20da%20Prova%20Digital%20no%20Processo,diante%20da%20aus%C3%AAncia%20de%20Regulamenta%C3%A7%C3%A3o&text=Resumo%3A,armazenamento%20de%20in%C3%BAmeros%20dados%20pessoais. Acesso em: 17 mar. 2023.

FERRAJOLI, Luigi. Direito e razão: teoria do garantismo penal. 3ª e.d. São Paulo/SP: RT, 2010.

FERREIRA, Círo Avila Machado. et al. A IOT (internet of things) no cenário brasileiro: suas vantagens e os principais desafios para sua implementação e expansão. **Revista Mythos**, Cataguases/MG, v. 13, n. 1, não paginado, jun. 2021. Disponível em: https://periodicos.unis.edu.br/index.php/mythos/article/view/438. Acesso em: 08 jan. 2023.

FGV EAESP – CENTRO DE TECNOLOGIA DE INFORMAÇÃO APLICADA. **33ª Pesquisa Anual do FGVcia: Uso da TI nas Empresas**. F. Meirelles. 2022. Disponível em: https://eaesp.fgv.br/producao-intelectual/pesquisa-anual-uso-ti. Acesso em 23 dez. 2022.

FLEISCH, Elgar et al. What is the internet of things? An economic perspective. **Economics, Management, and financial markets**, v. 5, n. 2, p. 125-157, 2010. Disponível em: https://www.ceeol.com/search/article-detail?id=267154. Acesso em: 27 dez. 2022.

FULLER, Paulo Henrique. et al. Lei anticrime comentada: artigo por artigo: inclui a decisão liminar proferida nas ADIs 6.298, 6.299 e 6.300. São Paulo/SP: Saraiva Educação, 2020.

GIACOMOLLI, Nereu José. **O devido Processo Penal**: abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica. São Paulo: Atlas, 2015.

GOUVEIA, Luís Manuel Borges. **Sociedade da informação: notas de contribuição para uma definição operacional**. Universidade Fernando Pessoa, Porto, Portugal, nov. 2004. Disponível em: http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf. Acesso em: 30 dez. 2022.

HOBSBAWM, Eric J. **Da Revolução Industrial Inglesa ao Imperialismo**. Tradução de Donaldson Magalhães Garschagen. 6ª ed. Rio de Janeiro/RJ: editora Forense Universitária, 2011. Disponível em: https://historiaeconomicageral.files.wordpress.com/2015/12/eric-hobsbawm-da-revoluc3a7c3a3o-industrial-inglesa-ao-imperialismo.pdf. Acesso em: 23 dez. 2022.

IGLÉSIAS, Francisco. **A Revolução Industrial**. 10ª ed. São Paulo/SP: editora Brasiliense, 1990. Disponível em: http://www.uel.br/laboratorios/lapege/pages/arquivos/Geografia%20da%20Industria/A%20revolucao%20industrial%20-%20Francisco%20Iglesias.pdf. Acesso em: 23 dez. 2022.

JEZLER JÚNIOR, Ivan; ESCHILETTI, Andrea Sartori. A cadeia de custódia das provas: o que não está nos autos, mas se aprisiona no mundo. In: GIACOMOLLI, Nereu José; STEIN, Carolina; SAIBRO, Henrique. **Processo penal contemporâneo em debate II.** 1 ed. Florianópolis: Empório do direito, 2017. p. 67-75. Disponível em: http://ibccrim.vpn.acelerati.com.br:5180/biblioteca/asp/prima-pdf.asp?codigoMidia=104341&iIndexSrv=1. Acesso em: 07 jul. 2023.

KIST, Dário José. **Prova digital no processo penal**. São Paulo: Leme/JH Mizuno, 2019.

KORESHOFF, Treffyn Lynch; ROBERTSON, Toni; LEONG, Tuck Wah. Internet of things: a review of literature and products. In: **Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration**. 2013. p. 335-344. Disponível em: https://dl.acm.org/doi/abs/10.1145/2541016.2541048. Acesso em: 27 dez. 2022.

LEAL, Hugo. **Projeto de Lei 4939/2020**. 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. Brasília:

Câmara dos Deputados, 15 out. 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2264367. Acesso em: 20 mar. 2023.

LEMOS, Diego Fontenele; CAVALCANTE, Larissa Homsi; MOTA, Rafael Gonçalves. A prova digital no direito processual brasileiro. **Revista Acadêmica Escola Superior do Ministério Público do Ceará,** Fortaleza/CE, v. 13, n. 1, p. 13-34, 2021. Disponível em: https://revistaacademica.mpce.mp.br/revista/article/view/147/137. Acesso em: 15 fev. 2023.

LESSA, Isabella Maria Baldissera; VIEIRA, Tiago Vidal. Crimes virtuais: análise do processo investigatório e desafios enfrentados. *In*: 5º Simpósio e Contemporaneidade nas ciências sociais, jun. 2017, Cascavel/PR. **Anais Eletrônicos.** Cascavel/PR: FAG, 2017. Disponível em: https://www.fag.edu.br/upload/contemporaneidade/anais/594c13e45d209.pdf. Acesso em: 11 jan. 2023.

LIMA, Renato Brasileiro de. **Manual de Processo Penal.** 8ª e.d. Salvador/BA: Jus-podivm, 2020.

LIMA, Renato Brasileiro de. **Pacote Anticrime:** Comentários à Lei n.º 13.964/19 – Artigo por Artigo. Salvador/BA: JusPodivm, 2020.

LOPES JÚNIOR, Aury. **Direito Processual Penal.** 17ª e.d. São Paulo/SP: Saraiva Educa, 2020.

LOPES JÚNIOR, Aury; ROSA, Alexandre Morais da. A importância da cadeia de custodia para preservar a prova penal. **Consultor Jurídico**, 16 jan. 2015. Disponível em: https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal. Acesso em: 05 jul. 2023.

LORENZO, Larissa Papandreus; SCARAVELLI, Gabriela Piva. Cibercrimes e a legislação brasileira. **Diálogos e Interfaces do Direito-FAG**, v. 4, n. 1, p. 104-122, 2021. Disponível em: https://dir.fag.edu.br/index.php/direito/article/view/83/66 . Acesso em: 09 jan. 2023.

MACHADO, Fernando Alves. **A cadeia de custódia e a prova penal digital**. Orientador: Diego Alan Schöfer Albrecht. 2022. Trabalho de Conclusão de Curso (Bacharel em Direito). Faculdade de Direito - Universidade Federal do Pampa, Sant'Ana do Livramento/RS: 2022. Disponível em: https://dspace.unipampa.edu.br/bitstream/riu/7179/1/FERNANDO_ALVES_MACHADO.pdf. Acesso em: 03 mar. 2023.

MACHADO, Leonardo Marcondes. Cadeia de Custódia da Prova Penal. In: CAMARGO, Rodrigo Oliveira de; FELIX, Yuri (Org). **Pacote Anticrime:** reformas processuais: reflexões críticas à luz da Lei 13.964/2019. Florianópolis/SC: Emais, 2020.

MACHADO, Michelle Moreira. Importância da cadeia de custódia para a prova pericial. **Revista Criminalística e Medicina Legal**. V. 1, n. 2, 2017, p. 8-12.

Disponível em: http://revistacml/.com.br/wp-content/uploads/2018/04/RCML-2-01.pdf. Acesso em: 17 jul. 2023.

MAGRINI, Eduardo. **Internet das Coisas**. Rio de Janeiro/RS: FGV Editora, 2018. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 28 dez. 2022.

MANZANO, Luíz Fernando de Moraes. **Prova pericial:** admissibilidade e assunção da prova científica e técnica no processo brasileiro. São Paulo: Atlas, 2011.

MARSHALL, Angus. **Digital forensics: digital evidence in Criminal Investigation**. WileyBlackwell. 2008.

MATIDA, Janaina. A cadeia de custódia é a condição necessária para a redução dos riscos de condenações de inocentes. **Boletim IBCCRIM**. São Paulo, v. 28, n. 331, 2020. Disponível em: https://www.ibccrim.org.br/publicacoes/edicoes/51/441. Acesso em: 07 jul. 2023.

MENDES, Carlos Hélder Carvalho Furtado. Dado informático como fonte de prova penal confiável(?): Apontamentos procedimentais sobre a cadeia de custódia digital. **Revista Brasileira de Ciências Criminais**. São Paulo, v. 161, [s.n.], p. 131-161, 2019. Disponível em: http://ibccrim.vpn.acelerati.com.br:5180/biblioteca/asp/primapdf.asp?codigoMidia=104930&iIndexSrv=1. Acesso em: 14 jul. 2021.

MENDES, Carlos Hélder Carvalho Furtado. **Malware do estado e processo penal:** a proteção de dados informáticos face à infiltração por software na investigação criminal. Orientador: Aury Lopes Júnior. 2018. Dissertação (Mestrado). Curso de direito – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre/RS, 2018. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/8537. Acesso em: 28 ago. 2023.

MINTO, Andressa Olmedo. **A prova digital no processo penal**. São Paulo/SP: Liberars, 2021.

MIZIARA, Raphael. Novas tecnologias e direito probatório: aspectos atuais sobre provas digitais. **Consultor Jurídico,** 8 maio 2022. Disponível em: https://www.conjur.com.br/2022-mai-08/raphael-miziara-aspectos-provas-digitais#_ftn4. Acesso em: 22 dez. 2022.

MOTA, Rafaella Ribeiro. **Blog como ferramenta de relacionamento e posicionamento de marca com o mercado consumidor:** um estudo de caso do blog “energia eficiente” da philips. 2010. Monografia (Bacharelado). Curso de Comunicação Social, Faculdade 7 de Setembro, Fortaleza, 2010. Disponível em: https://www.uni7.edu.br/recursos/imagens/File/publicidade/monografia/2010/Rafaela%20Mota.pdf. Acesso em: 02 jan. 2023.

NASCIMENTO, Natália Lucas. **Crimes cibernéticos**. 2016. Projeto de pesquisa. Curso de Processamento de Dados, Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, Assis/SP, 2016.

Disponível em: https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf. Acesso em: 12 jan. 2023.

NETO, Pedro Franco; LOPES, Vinicius Basso. Breves Considerações Sobre o Método de Valoração de Provas no Processo Penal e a Impossibilidade de Inversão do Ônus da Prova. **Revista de Ciências Jurídicas**, Paraná, v. 23, n. 1, p. 28-33, set. 2022. Disponível em: https://revistajuridicas.pgsskroton.com.br/article/view/10117. Acesso em: 15 mar. 2023.

NETTO, Luiz Ferraz. **A gaiola de Faraday**. [s.l], [s.d]. Disponível em: https://web.archive.org/web/20181202085448/http://www.feiradeciencias.com.br:80/sala11/11_47.asp. Acesso em: 21 set. 2023.

NUCCI, Guilherme de Souza. Provas no Processo Penal. 4ª e. d. São Paulo: Revista dos Tribunais, 2015. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/93039/provas_processo_penal_4.ed.pdf. Acesso em: 20 fev. 2023.

NÚMERO de Usuários de usuários do Instagram ultrapassa 2 bilhões e se aproxima do Facebook. **O Globo**, 26 dez. 2022. Disponível em: https://oglobo.globo.com/economia/tecnologia/noticia/2022/10/numero-de-usuarios-do-instagram-ultrapassa-2-bilhoes-e-se-aproxima-do-facebook.ghtml. Acesso em: 03 jan. 2023.

OLIVEIRA, Marcelo Ribeiro de. Cadeia de custódia digital: cuidados na preservação e especificação da metodologia. **Consultor Jurídico**, São Paulo/SP, mar. 2023. Disponível em: https://www.conjur.com.br/2023-mar-23/marcelo-oliveira-cadeia-custodia-digital-cuidados-metodo. Acesso em: 03 out. 2023.

OLIVEIRA, Vinicius Machado de. **ISO 27037 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital**. Academia de Forense Digital, [s. l.], jan. 2019. Disponível em: https://academiadeforensedigital.com.br/iso-27037- identificacaocoleta-aquisicao-e-preservacao-de-evidencia/. Acesso em: 27 ago. 2023.

O QUE é armazenamento na nuvem?. **Amazon Web Services**, 2020. Disponível em: https://aws.amazon.com/pt/what-is/cloud-storage/#:~:text=armazenamento%20em%20nuvem%3F-,O%20que%20%C3%A9%20o%20armazenamento%20em%20nuvem%3F,conex%C3%A3o%20de%20rede%20privada%20dedicada. Acesso em: 03 jan. 2023.

PACELLI, Eugênio. **Curso de processo penal.** 25. ed. São Paulo: Atlas, 2021.

PARODI, Lorenzo. A cadeia de custódia da prova digital à luz da Lei 13.964/2019. **Consultor Jurídico**, São Paulo/SP, jun. 2020. Disponível em: https://www.conjur.com.br/2020-jun-18/lorenzo-parodi-cadeia-custodia-provadigital?imprimir=1. Acesso em: 27 ago. 2023.

PARODI, Lorenzo. Cadeia de custódia das provas digitais vindas das nuvens, à luz do CPP. **Consultor Jurídico**, São Paulo/SP, abr. 2022. Disponível em:

https://www.conjur.com.br/2022-abr-10/lorenzo-parodi-cadeia-custodia-provas-digitais. Acesso em: 10 set. 2023.

PEREIRA, Larissa Maria Galvão. **Princípio da Oralidade no Processo Penal**. Orientadores: Néli Luiza C. Fetzner, Nelson Tavares e Mônica Areal. 2010. Artigo Científico (Pós-Graduação). Escola de Magistratura – Rio de Janeiro/RJ, 2010. Disponível em: https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2010/trabalhos_22010/larissapereira.pdf. Acesso em: 27 fev. 2023.

PERELMUTER, Guy. **Futuro Presente**. São Paulo/RS: Companhia Editora Nacional, 2019. Disponível em: https://doceru.com/doc/s0ne8e0. Acesso em: 22 dez. 2022.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4ª ed. São Paulo/SP: Saraiva, 2010.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. 1. ed. São Paulo: Marcial Pons, 2019.

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

PRESSE, France. Mais de um terço da população mundial não tem conexão com a internet, segundo a ONU. **G1**, 01 jan. 2021. Disponível em: https://g1.globo.com/tecnologia/noticia/2021/12/01/mais-de-um-terco-da-populacao-mundial-nao-tem-conexao-com-a-internet-segundo-a-onu.ghtml. Acesso em: 03 jan. 2023.

RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Almedina, 2017.

ROCHA, Adriano Aparecido. **Cibercriminalidade os crimes cibernéticos e os limites da liberdade de expressão na internet**. 2017. Monografia (Bacharelado). Curso de direito, Faculdade de Ensino Superior e Formação Integral, Garça/SP, 2017. Disponível em: https://www.faef.br/userfiles/files/23%20-%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20NA%20INTERNET.pdf. Acesso em: 10 jan. 2023.

ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. **Blog Ampla Defesa**. 2013. Disponível em: https://ampladefesa.wordpress.com/2013/08/25/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-7372012/. Acesso em: 10 jan. 2023.

RODRIGUES, Benjamim Silva, ob. cit., Coimbra Editora, 2009, p. 726. *In*: CANCELA, A. G. L. **A prova digital**: os meios de obtenção de prova na Lei do Cibercrime. Orientador: Sónia Mariza Florêncio Fidalgo. 2016. Dissertação (Mestrado em Direito) - Universidade de Coimbra, Coimbra, 2016. Disponível em: https://estudogeral.sib.uc.pt/bitstream/10316/31398/1/A%20prova%20digital.pdf. Acesso em: 10 fev. 2023.

ROSA, Fabrizio. Crimes de Informática. Campinas: Bookseller, 2002. P. 53.

ROSSINI, Augusto. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica Editora, 2004.

SANTOS, Adriano José Souza; BORGES, André Felipe Miranda; RODRIGUES, Gustavo Luis Mendes Tupinambá. A cadeia de custódia na coleta da prova digital de acordo com a Lei 13.964/2019: dos seus artigos 158-A ao 158-F. **Revista Científica Multidisciplinar ISSN 2675-6218**, [s.l], v. 2, n. 8, p. e28612-e28612, 2021. Disponível em: https://recima21.com.br/index.php/recima21/article/view/612. Acesso em: 10 set. 2023.

SARNEY, José. **Projeto de Lei 8.045/2010**. Código de Processo Penal. Revoga o Decreto-lei nº 3.689, de 1941. Altera os Decretos-lei nº 2.848, de 1940; 1.002, de 1969; as Leis nº 4.898, de 1965, 7.210, de 1984; 8.038, de 1990; 9.099, de 1995; 9.279, de 1996; 9.609, de 1998; 11.340, de 2006; 11.343, de 2006. Brasília: Câmara dos Deputados, 22 dez. 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=49026. Acesso em: 20 mar. 2023.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução: Daniel Moreira Miranda. São Paulo/RS: Edipro, 2016.

SOARES, Matias Gonsales. A Quarta Revolução Industrial e seus possíveis efeitos no direito, economia e política. **Migalhas**, 2018. Disponível em: https://www.migalhas.com.br/arquivos/2020/6/B86DDA9403078E_AQuartaRevolucaoIndustrialeseu.pdf. Acesso em: 28 dez. 2022.

SOUZA, Débora da Paz. **Proteção de dados e o processo penal**: desafios e parâmetros da cadeia de custódia da prova digital. Orientador: Ney de Barros Bello Filho. 2021. Trabalho de Conclusão de Curso (Bacharel em Direito). Faculdade de Direito – Universidade de Brasília, Brasília/DP, 2021. Disponível em: https://bdm.unb.br/handle/10483/28900. Acesso em: 10 mar 2023.

THE People vs O. J. Simpson (temporada 1). American Crime Story [seriado]. Direção: Ryan Murphy e Anthony Hemingway. Produção: Scott Alexander, Dante Di Loreto, Brad Falchuk, Nina Jacobson, Larry Karaszewski, Ryan Murphy, Brad Simpson e Alexis Martin Woodall. Estados Unidos: American Broadcasting Company, 2016, 1 DVD, son. color. Dublado. Port. 1 DVD. Disponível em: https://www.starplus.com/pt-br/series/american-crime-story/1vo8c9OAjanv. Acesso em: 03 jul. 2023.

VAZ, Denise Provazi. **Provas digitais no processo penal**: formulação do conceito, definição das características e sistematização do procedimento probatório. Orientador: Antonio Scarance Fernandes. 2012. Tese (Doutorado). Curso de direito - Universidade de São Paulo/SP, São Paulo/SP, 2012. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/publico/Denise_Provasi_Vaz_tese_integral.pdf. Acesso em: 21 dez. 2022.

VELLOSO, Jean Pablo Barbosa. **Crimes Informáticos e Criminalidade Contemporânea**. 2015. Monografia (Bacharelado). Curso de Direito, Universidade Luterana do Brasil, Gravataí/RS, 2015. Disponível em: https://www.conteudojuridico.com.br/consulta/Monografias-TCC-Teses-E-Book/45359/crimes-informaticos-e-criminalidade-contemporanea. Acesso em: 30 dez. 2022.

VIANA, Bernardo. O mar de dados virou um oceano e não para de crescer. mas nem tudo é aproveitado. **Insper**, 22 dez. 2021. Disponível em: https://www.insper.edu.br/noticias/o-mar-de-dados-virou-um-oceano-e-nao-para-de-crescer-mas-nem-tudo-e-aproveitado/. Acesso em: 03 jan. 2023.

WERTHEIN, Jorge. A Sociedade da Informação e seus desafios. **Ciência da Informação,** Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000. Disponível em: https://www.scielo.br/j/ci/a/rmmLFLLbYsjPrkNrbkrK7VF/?lang=pt&format=pdf. Acesso em: 30 dez. 2022.

ZANIOLO, Pedro Augusto. **Crimes Modernos**: O impacto da tecnologia no direito. 4º ed. Salvador: JusPodivm, 2021.