INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA – IDP
ESCOLA DE DIREITO DO BRASIL – EDIRB

MESTRADO PROFISSIONAL INTERDISCIPLINAR EM DIREITO, JUSTIÇA E DESENVOLVIMENTO

RODRIGO PINHEIRO FÉRES

USO DE INFORMAÇÕES ARMAZENADAS EM MEIO DIGITAL NO PROCESSO PENAL

SÃO PAULO

2021

RODRIGO PINHEIRO FÉRES

USO DE INFORMAÇÕES ARMAZENADAS EM MEIO DIGITAL NO PROCESSO PENAL

Dissertação de Mestrado, desenvolvida sob a orientação do Professor Alamiro Salvador Netto apresentado para obtenção do Título de Mestre em Direito, Justiça e Desenvolvimento.

SÃO PAULO

2021

RODRIGO PINHEIRO FÉRES

USO DE INFORMAÇÕES ARMAZENADAS EM MEIO DIGITAL NO PROCESSO PENAL

Dissertação de Mestrado apresentada ao Programa de Mestrado Interdisciplinar Profissional em Direito, Justiça e Desenvolvimento do IDP, como requisito para obtenção do título de Mestre em Direito, Justiça e Desenvolvimento.

13 de dezembro de 2021.

BANCA EXAMINADORA

_____

Prof. Alamiro Velludo Salvador Netto

_____

Prof.ª Maria Edevalcy Pinto Marinho

_____

Prof.ª Jéssica Raquel Sponchiado

SUMÁRIO:

RESUMO:

As informações preservadas em meio digital são caracterizadas pela imaterialidade, volatilidade, fragilidade e dispersão. Os dados podem ser espoliados, sujeitos a degradação por incidência de elementos externos ou adulterados, manipulados pelos agentes que os têm acesso. A própria possibilidade de acessar e trabalhar dados de maneira legitima não impede a distorção ocasionada pela ignorância técnica sobre a informação adquirida. Nesse contexto, observa-se necessidade de um tratamento diferenciado às provas preservadas em meio digital dentro do processo penal, norteando sua admissibilidade em juízo pelas norteado pelas suas características intrínsecas. O tema é enfrentado pelo método hipotético-dedutivo, através de revisão bibliográfica e sob a ótica do garantismo penal de Ferrajoli. Adota-se como critério de validade da prova penal o controle epistemológico proposto por Geraldo Prado, condicionando sua aceitação em juízo a preenchimento de requisitos de Sumidade e Desconfiança.

Palavras-chave: Processo Penal; Prova; Prova Digital; Controle Epistemológico.

ABSTRACT:

Information preserved in digital media is characterized by immateriality, volatility, fragility, and dispersion. Data can be plundered, subject to degradation by the incidence of external elements or be tampered with, manipulated by the agents who have access to them. The very possibility of accessing and working with data in a legitimate way does not prevent the distortion caused by technical ignorance about the information acquired. In this context, there is a need for a differentiated treatment of evidence preserved in digital media within the criminal procedure, guiding its admissibility in court by its intrinsic characteristics. The theme is dealt with the hypothetical-deductive method, through bibliographic review and from the perspective of Ferrajoli's criminal guarantee theory. The epistemological control proposed by Geraldo Prado is adopted as a standard for validity of criminal evidence, conditioning its admission in court to the fulfilment of Worthy and Distrust requirements.

Keywords: Criminal Procedure; Proof; Digital Evidence; Epistemological Control.

INTRODUÇÃO

A utilização de meios eletrônicos no ambiente jurídico-processual não é novidade, porém não se pode afirmar que todos os desafios dos avanços tecnológicos foram vencidos.

Na década de 1980 foram disponibilizados para uso os primeiros computadores domésticos, que na década seguinte teriam sua capacidade expandida pelo acesso difundido à *internet*. Esses avanços tecnológicos foram percursores da revolução na forma de armazenamento e comunicação de dados ocasionada pela profusão de *smartphones*, *notebooks* e *tablets*. (QUITO, 2020, p. 162)

Tais inovações foram acompanhadas de uma super documentação do cotidiano. As pessoas carregam *smartphones* capazes de registrar fatos sem maiores dificuldades, razão de quase todo conflito ser acompanhado de algum registro audiovisual. Há o catálogo de entra e saída de pessoas em edifícios e o sistema de GPS pode localizar indivíduos no globo com uma margem de erro de 5 metros (CABRAL, 2020, p. 94).

O excesso de informações disponibilizada pela via digital e sem barreiras físicas leva a realidade semelhante a ficções distópicas. Edward Snowden expôs em 2013 que a NSA realizava vigilância em massa dos usuários na *internet* através da exploração de vulnerabilidades de sistemas e *malwares* para coletar dados (THE INTERCEPT, 2019).

A evolução tecnológica não diminuiu o ritmo e já se apresenta a próxima era no horizonte. Há projeções do impacto da implementação da *internet* das coisas na proteção da privacidade, apontando que o potencial de 100 bilhões de dispositivos inteligentes conectados entre hão de gerar uma quantidade imensurável de dados coletada (MAGRANI e ABRAHÃO, 2019, p.169-170).

Com o desenvolvimento de novas tecnologias, fica à disposição das partes novos meios de provas, não necessariamente previstos na legislação, contudo também não proibidos por ela. Nessas situações, incorporam-se ao processo através da analogia com os meios de prova convencionais.

Entretanto, as especificidades do meio apresentado não se adequam completamente ao procedimento análogo inicialmente utilizado. Nesse contexto, atenta-se especialmente às informações preservadas em arquivos digitais. Elas são expressas através do processamento de dados contidos nos arquivos, sendo

passíveis de falhas e adulterações no momento que a interpretação dos dados é realizada pelo agente intermediário.

Deste modo, esse trabalho visa entender se há necessidade de um tratamento diferenciado às provas digitais no processo penal.

Procurando entender as especificidades da utilização de informações extraídas de arquivos digitais no processo penal, será analisada sua natureza jurídica enquanto meio de prova, sob a ótica garantista, ainda que ressalvada as ponderações pragmáticas relativas à busca da verdade na atividade probatória e o contraponto da eficiência no processo penal.

A informatização já é algo presente no cotidiano processual judiciário, havendo previsão legal do processo digital desde 2006, com a Lei 11.419/06 (BRASIL, 2006). Porém, a adoção da informatização no processo não se correlaciona diretamente com o domínio do meio digital pelos operadores do direito, seja no plano nacional ou internacional.

Em 2016, o jovem Lukas da Silva Fortuna foi preso em flagrante por supostamente estar comercializando drogas próximo a uma estação de metrô no Rio de Janeiro, estando em uma motocicleta acompanhado de comparsa que dirigia outra motocicleta.

Lukas teria utilizado uma arma de fogo contra os policiais quando foi abordado no sinal de trânsito, justificativa utilizada pelos agentes ao realizar disparos com um fuzil nas pernas dele. O suposto comparsa teria fugido, sendo apreendido com Lukas uma mochila com quantidade expressiva de maconha.

Lukas teve contato com o pai na delegacia, que alegou ser inocente e que tinha sido abordado em outro local sozinho e sem nada ilícito. O pai obteve uma gravação da câmera de segurança de um bar na localização da abordagem apontada pelo filho, constatando que o jovem havia ser abordado sozinho, parado na calçada com sua motocicleta, aguardando a chegada de alguém, sem portar qualquer mochila.

A polícia estava em automóvel descaracterizado e abordou Lukas exigindo que ele levantasse sua camisa para mostrar que não estava armado. Com medo da abordagem, o jovem correu, sendo perseguido e detido pelos policiais após o disparo de fuzil atingi-lo na perna (RANGEL, 2020, p. 103-104).

Não houve impugnação por parte do Ministério Público sobre a autenticidade das gravações, mas o juízo ignorou as imagens juntadas, condenando Lukas. Ele foi absolvido em segundo grau, por apenas maioria dos votos pois um dos

desembargadores entendeu que deveria ser mantida a condenação na medida que “a apreensão de mais de 04 quilos de maconha, a fuga do réu do local, ferido por tiros dos policiais, e o silêncio do mesmo em sede policial e em juízo, sendo irrelevante as imagens das câmeras, pois de péssima qualidade” (BRASIL, 2018).

No âmbito do Tribunal Penal Internacional (TPI), há precedentes do uso de provas digitais, porém não houve enfrentamento conclusivo sobre a matéria.

Em 2012, no caso Al-Mahdi, foram utilizadas gravações de áudio encontradas na *internet* contendo declarações dos membros do grupo terrorista que o réu era parte, além de diversas gravações de vídeo divulgados pela população do Mali que mostravam o momento da destruição dos monumentos históricos e religiosos pelos quais ele respondia como crime de guerra.

Na ocasião, a acusação foi diligente em verificar a autenticidade das gravações, utilizando peritos para georreferenciar as localizações e estimar o período que foram realizadas. Porém, a Corte não decidiu acerca da admissibilidade na ocasião pois a defesa não questionou as provas (NASCIMENTO, 2020, p. 113).

Houve também a emissão de mandado de prisão contra Al Werfalli, em 15 de agosto de 2017, fundamentado em vídeos divulgados *online* que supostamente revelavam sete execuções orquestradas pelo réu na Líbia (NASCIMENTO, 2020, p. 112). Apesar de fundamentar o mandado de prisão, também não houve até o momento decisão final sobre a admissibilidade das provas para a condenação.

Os arquivos digitais fornecem informações através do processamento de dados neles contidos (MASSON, 2017, p. 672). Pressupondo a dinâmica exposta, há sempre um agente intermediário interpretando os dados alocados para fornecimento da informação. Esse agente, seja, por exemplo, um *software*, *hardware* ou uma plataforma *online*, é passível de sofrer com falhas e vulnerabilidades, podendo ocorrer erro ou manipulação na interpretação dos dados que levem a adulteração da informação fornecida.

Em 2015, após um ataque terrorista em San Bernardino, Califórnia, o FBI solicitou a Apple possibilitasse o acesso de autoridades ao seu sistema operacional através de mecanismo de acesso excepcional, ante a dificuldade de extrair os dados contidos no Iphone 5c apreendido de um dos investigados.

Como tiveram acesso aos dados do celular com ajuda de terceiros, o FBI desistiu de interpelar judicialmente a Apple para que cumprisse a demanda. À época, a empresa havia recusado o pedido sob a alegação que a inserção de tal mecanismo

de acesso excepcional ocasionaria um grave comprometimento de seu sistema de segurança (LIGURI FILHO, 2019, p. 93).

Entra em discussão o limite da intervenção investigativa em prol da segurança coletiva contrapondo a segurança dos sistemas informáticos que, além da proteção individual, também tem escopo de proteção coletiva.

Ainda, há de se ponderar a busca pela verdade como princípio do processo penal e a necessária pessoalidade da responsabilização. Sendo vedada a imputação de modo objetivo, ante a ausência de dolo e culpa, a própria autoria da alocação original dos dados também é questionável se não acompanhada de outros elementos que a corroborem quando não realizadas dentro de um sistema de autenticidade de credenciais robusto.

Os próprios sistemas processuais eletrônicos (a título de exemplo, o *e-SAJ* e o PJe) atentam-se a essa dinâmica, exigindo identificação com certificado digital para inserir dados e criando um mecanismo para conferir a veracidade das informações extraídas de seus sistemas.

O enfrentamento da natureza das provas obtidas ou originadas do meio eletrônico é fundamental para sua correta valoração sob a égide dos princípios constitucionais que norteiam o processo penal.

Além de se extrair a plenitude das informações acostadas no arquivo digital e atestar sua validade, vencer a lacuna de compreensão do meio é imprescindível para o operador do Direito.

Considerando ainda a segurança jurídica, o caso recente da Dinamarca representa a necessidade de o problema ser enfrentado. Em 3 de março de 2019 foi descoberta uma falha no sistema que converte dados das empresas de telefonia para uso como prova de localização de pessoas no local do crime, o que levou a necessidade de revisar 10.000 condenações devido a erros nos dados de rastreamento (THE LOCAL DENMARK, 2019). Não existem estatísticas quantas sentenças foram proferidas com base somente nesses dados, porém, pelo menos 29 pessoas foram soltas em decorrência do erro (KIRO7, 2019). A análise correta do meio de prova para seu uso poderia ter evitado tamanho transtorno.

Trazendo um exemplo mais próximo à realidade judiciária brasileira, a Operação *Spoofing* trouxe uma discussão expansiva sobre a admissibilidade de prova ilícita em favor da defesa.

No caso, a ilicitude se dá justamente pela impossibilidade de atestar a integridade das informações extraídas a partir da invasão ilegal de celulares de diversas autoridades (JORNAL NACIONAL, 2021).

Assim, apesar de pacífico o uso de prova ilícita em favor do réu, a possibilidade de utilizar informações não confiáveis abre espaço para fraudes processuais baseadas na ignorância técnica dos julgadores.

Ante as considerações expostas, é necessário observar as especificidades das provas digitais, seja uma captura de imagem de uma postagem em rede social, a gravação audiovisual de um fato ou informações de localização fornecidas por um celular, ressalvando que a correta determinação origem desses dados e seu processamento em informação são fundamentais para sua validade.

As provas são o meio pelo qual é possível reconstruir um fato passado (LOPES JÚNIOR, 2019, p. 341) para conhecimento instrutivo do juiz. Dentro da dinâmica processual, provas podem também ser definidas como quaisquer elementos que, obedecidos os requisitos de legalidade e respeitado o contraditório, servirão para influenciar a decisão do juiz.

Enquanto instrumento de retrospeção, a prova digital deveria ser objeto de perícia, não tratado como mero documento, pois existem elementos ocultos em sua dinâmica que são essenciais para aproximação da realidade. Somente por intermédio atuação de profissional técnico é possível revelar todas as informações relevantes no armazenamento digital de vestígios.

Por outro lado, do ponto de vista pragmático, o excesso de formalidade atribuído à admissibilidade de informações armazenadas em meio digital apresentadas em juízo poderia gerar uma onerosidade terrível ao processo, limitando sua efetividade e aumentando a impunidade sob a escusa abusiva de uma estrita imposição de certeza de revelar a verdade absoluta.

Também há de ser considerado que os arquivos digitais em regra são gerados em plataformas privadas, motivo pelo qual a viabilidade dessas perícias é incerta, indo além de simples conhecimento técnico para averiguação de toda a cadeia envolvida no processamento da informação.

Ainda, tratando da privacidade no ambiente virtual, seja o uso de dispositivos informáticos ou acesso à *internet*, a Constituição Federal traz especial proteção a intimidade e a vida privada. Mesmo que as interações sejam realizadas por intermédio plataformas abertas ao público, entende-se temerário a propositura de instituições que

restrinjam a liberdade e privacidade dos usuários em nome de robustecer a confiabilidade probatória das informações lá contidas.

A permeabilidade da privacidade no âmbito virtual é sorrateira. Uma imensa quantidade de dados é deixada a cada interação, sendo possível através de recursos informáticos concatenar e devassar informações privadas dos indivíduos que não seria possível sob o abrigo do domicílio físico (PRADO, 2020, p. 55).

Questões pertinentes a atividade probatória em meio digital clamam especial atenção a permeabilidade da vida privada e intimidade consequentes do uso da *internet*, quer considerando ambientes abertos ao público, como redes sociais, ou estritamente privados, em aplicativos de troca de mensagens.

Assim, além da função legitimadora, o balizamento da atividade probatória também se propõe a não justificar imposição de restrições as interações em ambientes virtuais. Parte-se do princípio de que é injustificável impor restrições prévias à liberdade de um indivíduo em nome de uma maior confiabilidade em eventual colheita de provas caso este venha a ser um potencial delinquente.

Postas tais considerações, adotando o método hipotético-dedutivo, através de revisão bibliográfica, propõe-se enfrentar a questão balizado a ideia de procedimento justo em preceitos norteadores e sob a ótica da teoria do garantismo penal de Luigi Ferrajoli (2002), trazendo especial atenção aqueles axiomas que expressam garantias relativas ao processo.

Quanto ao critério de validade e confiabilidade da prova, utiliza-se o sistema de controle epistêmico da atividade probatória exposto por Geraldo Prado, exigindo-se que o arquivo digital utilizado como prova preencha os requisitos de Sumidade e Desconfiança (PRADO, 2014).

Do ponto de vista institucional, impõem-se a presunção de inocência no tratamento da atividade probatória e, para tanto, criteriosa limitação a vigilância estatal na vida privada. Deste modo, a confiabilidade e validade da prova digital não podem justificar a restrição da liberdade individual em prol de persecução penal.

Inicialmente, procurou-se responder à pergunta pelo viés da busca pela aproximação com a realidade, ante o princípio da busca da verdade real. Porém, tal ponto de vista limitou a pesquisa a âmbitos rasos de discussão de cadeia de prova e, ironicamente, excessivo formalismo na produção probatória.

A segunda ideia rejeitada foi utilizar conceitos neoinstitucionalistas (North e Acemoglu) para tratar de liberdade e contrapor medidas que visam trazer vigilância

como regra para tratamento da conduta das pessoas *online*, contrariando garantias constitucionais, e as consequências na atividade probatória. O tópico dispersou o foco da problematização proposta, adentrando questões mais afins a seara de liberdade de expressão e menos em questões processuais.

Então, foi delimitado o escopo em três frentes, articulando conceitos a partir da teoria até alcançar questões mais práticas, com fundamentação subsequente capítulo a capítulo.

O capítulo 1 situa o conceito de processo justo a ser utilizado como parâmetro para enfrentamento do problema compatível com o sistema processual penal brasileiro. Busca elencar o escopo das garantias constitucionais relacionadas ao processo penal, estabelecendo critérios para um processo justo que será utilizado como elemento norteador para os capítulos subsequentes.

Propõem-se inicialmente o modelo garantista de Ferrajoli como critério norteador axiomático, procedendo a defender sua compatibilização com o sistema jurídico constitucional brasileiro. É enfrentado a aparente contradição das disposições quanto ao ônus da prova e a iniciativa probatória pelo juízo, bem como um sistema de garantias e a eficiência no processo penal.

O capítulo 2 é voltado ao papel da prova no processo penal e a construção da verdade processual. Volta-se para esclarecer a função da prova sua relação com o objetivo do processo penal.

É delimitada a dinâmica processual a qual se insere a prova dentro do exercício do contraditório e elemento de convicção do juízo. Também traz ponderações sobre a construção de verdade através do procedimento judicial e os limites à capacidade de conhecimento de fatos relevantes ao esclarecimento de infrações.

O capítulo 3 é voltado a prova digital propriamente dita, aos possíveis limites técnicos/práticos de seu controle de validade técnico e um limiar de riscos aceitáveis relacionados a prova digital.

Inicia-se conceituando o que é prova digital, passando a elucidar a dinâmica de armazenamento de informações em meio digital. Serão abordadas questões sobre a extração de dados e a perícia técnica sobre dispositivos informáticos, bem como o controle epistemológico das provas digitais e consequente segurança de idoneidade das informações apresentadas. Segue o capítulo com ponderações sobre a

acessibilidade de dados, a qualidade dos dados extraídos e sistema de autenticação digitais.

Por fim, a conclusão da dissertação visa ser propositiva, apresentando um padrão de enfrentamento das provas digitais justo e eficiente, obedecendo os axiomas apresentados no primeiro capítulo, se atendo a função exposta no segundo capítulo e dentro do padrão probatório aceitável delimitado no terceiro.

1. GARANTIAS PROCESSUAIS E O PROCESSO JUSTO

A persecução penal se legitima pela coerência entre a resposta dada pelo Estado à sociedade quanto a determinado fato delituoso e o justo tratamento daquele que seja investigado e eventualmente penalizado, dado ao seu monopólio de poder.

O exercício do poder de penalizar do Estado submete-se a ritos e limites para proteger o indivíduo de eventual arbitrariedade, porém, também não há razoabilidade se estes procedimentos e restrições não permitirem o Estado coibir infrações de maneira minimamente eficiente.

Se faz necessário determinar um parâmetro basilar de procedimento justo, cujos valores sejam claros e permitam com segurança delimitar limites à atividade probatória.

O modelo garantista de Ferrajoli (2002) traz a premissa de assegurar o máximo grau de racionalidade e confiabilidade do juízo, limitando o poder punitivo do Estado e resguardando o indivíduo de suas arbitrariedades.

Ferrajoli preserva o cerne do Positivismo Jurídico em sua proposta, entendendo direito e moral como institutos separados. A norma jurídica é tida como um produto artificial de origem social, construída pela autoridade competente e organizada em graus hierárquicos de acordo com critérios formais (ZANON JUNIOR, 2015).

Assim, há um ponto de vista interno jurídico e um ponto de vista externo social do ordenamento, operando na lógica interna de validade e invalidade normativa e a lógica externa de valoração moral de justo ou injusto,

A epistemologia garantista é constituída pelo convencionalismo penal e o cognitivismo processual, e deles se extraem 10 axiomas formadores do sistema garantista de direito (FERRAJOLI, 2002, p. 30-33, 72).

O elemento convencionismo penal, regido pelo princípio da legalidade estrita, condiciona a determinação abstrata de um desvio punível ao caráter formal do critério de definição e o carácter fático daquelas hipóteses definidas. Somente pode ser considerado um crime o que a lei o define como tal, ficando o juiz submisso a lei, não havendo liberdade para estabelecer sanção fundada em seu entendimento sobre determinado ato ser valorado negativamente. Ainda, a definição dos desvios puníveis deve se direcionar a questões objetivas e fáticas, possibilitando determinar seu campo de aplicação de forma exclusiva e exaustiva, em contraponto a uma delimitação de figuras subjetivas direcionadas criminalização do autor (FERRAJOLI, 2002, p. 31).

No âmbito da determinação concreta do delito punível, o cognitivismo processual rege-se pela égide da estrita jurisdicionariedade, que o condiciona a verificabilidade ou refutabilidade das hipóteses acusatórias e um procedimento de comprovação empírica também permitindo verificação ou refutação daquilo apresentado. Deste modo, estabelece-se um modelo de processo penal que conhece o fato previsto em lei como delito punível através de alegações de fato e de direito sujeitas a comprovação empírica, sendo elas consequentemente delineadas como verdade ou falsidade processual (FERRAJOLI, 2002, p. 32-33).

Tal controle epistemológico, em especial o modelo de cognitivismo processual, motiva atenção à atividade probatória virtual. Se o procedimento penal deve expressar confiabilidade e racionalidade, a comprovação empírica da verdade ou falsidade das informações alocadas em meios informáticos deve ser adequada as características deste.

Dos elementos epistemológicos apresentados, extraem-se os 10 axiomas formadores do sistema garantista penal, expressando cada um deles respostas a questões de intervenção penal e respectivas garantias, sendo eles divididos em três grandes grupos: aqueles relativos a questões da punição e garantias relacionadas à pena; aqueles pertinentes a questões de proibição e garantias referentes ao delito ; e, por fim, aqueles que versam sobre o julgamento e garantias processuais (FERRAJOLI, 2002, p. 75).

Em primeiro momento, considerando a natureza probatória do problema aqui enfrentado, o último grupo de axiomas é apropriado ao balizamento da atividade e o tratamento daquele está ou potencialmente estará sujeito ao procedimento de conhecimento penal.

O sétimo axioma, *nulla culpa sine judicio* traz o princípio da jurisdicionariedade, expressando a submissão do juízo a lei, tanto em sentido estrito quanto lato. Em sentido estrito, a observância de procedimentos e garantias previstos para a cognição do juízo de um sistema acusatório. Já no sentido lato, referente à necessidade de respeitar a imunidade do indivíduo contra arbitrariedades de sua liberdade, a reserva de jurisdição para imputar punição e decidir sobre a imputação de um fato delituoso, e a presunção de inocência, garantindo que nenhum indivíduo será tratado como culpado antes da conclusão da cognição do suposto fato delituoso por um juízo legítimo (FERRAJOLI, 2002, p. 433).

A presunção de inocência é a escolha do sistema garantista pela imunidade do inocente ao custo da impunidade de algum culpado, na medida que cria um sistema eficiente, mas propositalmente não absolutamente eficaz, ante a necessária coesão entre liberdade e segurança. Exigindo que a atuação estatal seja corretamente legitimada dentro da lei, busca aqui privilegiar a segurança do cidadão de não ter sua vida devassada e sua liberdade tolhida por eventuais arbítrios das autoridades estatais. Deste modo, o sistema deve funcionar punindo a maioria dos culpados, resguardando uma certa margem de erro em prol da segurança e liberdade (FERRAJOLI, 2002, p. 441-442).

Ainda, ressalva-se que a submissão do juízo a lei também implica na não derrogação do juízo. Quando provocado por uma ação penal o julgamento é indeclinável e infungível, o juiz não pode se furtar de julgar qualquer que seja o assunto e a atividade cognitiva do juízo monopoliza a repressão penal.

O princípio acusatório, expresso pelo 8º axioma *nullum judicium sine accusatione*, traz a premissa de separação dos sujeitos com função judicante daqueles que tem função postuladora, além da garantia do imputado se defender das acusações postuladas, em ato prévio e delimitador do juízo. Assim, estabelece-se a figura do juiz separado da acusação, distante e desinteressado. O distanciamento do juiz estabelece a paridade da defesa com a acusação, sem que o órgão acusatório tenha qualquer poder sobre o acusado, ficando suas alegações sujeitas ao ônus probatório e o contraditório (FERRAJOLI, 2002, p. 450).

Assim, no procedimento cognitivo penal, fica a acusação obrigada a provar suas alegações com provas idôneas e convincentes, ficando suas hipóteses sujeitas ao livre desenvolvimento do conflito pela defesa, sob o véu da presunção de inocência. Essa obrigação e garantia são expressos pela conjugação do 9º e do 10º axioma: *nulla accusatio sine probatione* (princípio do ônus da prova) e *nulla probatio sine defensione* (princípio do contraditório).

A pertinência da escolha deste referencial teórico é a razoabilidade dos parâmetros por ele estabelecidos para enfrentar o problema posto, além de que os princípios garantistas apresentados estão inseridos no sistema penal constitucional brasileiro. A escolha pelo um modelo garantista é expresso pela previsão de garantias judiciais como direitos fundamentais no corpo constitucional e recentemente, reiterando a acepção da separação da parte acusatória e do juiz, foi incluído o artigo 3-A no Código de Processo Penal: “processo penal terá estrutura acusatória, vedadas

a iniciativa do juiz na fase de investigação e a substituição da atuação probatória do órgão de acusação" (BRASIL, 1941).

Nucci (2020, p. 114) defende que a Constituição Federal de 1988 apenas aponta para o sistema acusatório, porém a imposição das regras processuais penais parte do Código de Processo Penal, que implicaria na adoção de um sistema acusatório mitigado após a referida alteração legislativa.

Não obstante a posição aventada, ela não se compatibiliza com o sistema posto, sendo mera reiteração heurística de justificação daqueles preceitos pré-constitucionais expressados pelo sistema processual penal. A existência de uma polícia judiciária constitucional ou a produção de provas por iniciativa do juiz não são características que mitigam a aplicação do princípio acusatório, a separação entre acusação e julgador.

Tal postulado contradiz as demais garantias constitucionais expressas. Ainda que não se coloque como absolutas, não há espaço para aceitar a primazia da razão do Estado em uma democracia.

A soberania de uma razão de Estado reintroduz a figura do réu como inimigo, não como sujeito de direitos, e reduz a sociedade a mero substrato populacional homogêneo, ignorando a complexa e diversa realidade dos movimentos sociais (PRADO, 2014, p. 28).

O princípio da jurisdicionariedade enquanto submissão do juízo à lei é destacada no artigo 1º do Código Penal e reiterada como princípio constitucional no inciso XXXIX, do artigo 5º da Carta Magna brasileira "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (BRASIL, 1988), inclusive impondo-se a necessidade de fundamentação das decisões do Juízo, nos termos do artigo 93, inciso IX, também da Constituição Federal:

> Todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação (BRASIL, 1988)

Ainda o artigo 5º, da Constituição Federal trás garantias como a inadmissibilidade das provas obtidas por meios ilícitos e o remédio constitucional do *Habeas Corpus* contra arbitrariedades e ilegalidades:

> LXV - a prisão ilegal será imediatamente relaxada pela autoridade judiciária; [...]

> LXVIII - conceder-se-á habeas corpus sempre que alguém sofrer ou se achar ameaçado de sofrer violência ou coação em sua liberdade de locomoção, por ilegalidade ou abuso de poder;(BRASIL, 1988)

A presunção de inocência encontra-se no nosso ordenamento com a conjugação do inciso LVII, do referido artigo 5º, “ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória” (BRASIL, 1988) com a previsão do artigo 8º, item 2, do Pacto de São José da Costa Rica (Convenção Interamericana de Direitos Humanos) “Toda pessoa acusada de delito tem direito a que se presuma sua inocência enquanto não se comprove legalmente sua culpa“ (BRASIL, 1992).

A reserva de jurisdição também se encontra no recorrentemente referido artigo 5º, resguardando o monopólio judicial para decidir sobre a aplicação de pena e restrição da liberdade:

> LIII - ninguém será processado nem sentenciado senão pela autoridade competente;
> LIV - ninguém será privado da liberdade ou de seus bens sem o devido processo legal; [...]
> LXI - ninguém será preso senão em flagrante delito ou por ordem escrita e fundamentada de autoridade judiciária competente, salvo nos casos de transgressão militar ou crime propriamente militar, definidos em lei (BRASIL, 1988)

A Constituição Federal no artigo 129, inciso I, institui o Ministério Público e sua função enquanto órgão acusatório de promover as ações penais públicas, estabelecendo a separação do órgão acusatório oficial da estrutura do juízo, assim como a vedação ao juízo de exceção estabelecida no artigo 5º, inciso XXXVII, também da Carta Magna (BRASIL, 1988), bem como a garantia disposta no artigo 8º, item 1, do Pacto de São José da Costa Rica:

> Toda pessoa tem direito a ser ouvida, com as devidas garantias e dentro de um prazo razoável, por um juiz ou tribunal competente, independente e imparcial, estabelecido anteriormente por lei, na apuração de qualquer acusação penal formulada contra ela, ou para que se determinem seus direitos ou obrigações de natureza civil, trabalhista, fiscal ou de qualquer outra natureza. (BRASIL, 1992)

Apesar do direito ao contraditório ser evidente, expresso tanto garantia constitucional do inciso LV, do artigo 5º “aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerente” (BRASIL, 1988), quanto pela previsão de que a convicção do juiz deverá ser formada por apreciação da prova produzida em contraditório judicial disposta no artigo 155 do Código de Processo Penal (BRASIL,

1941) o princípio do ônus da prova da acusação encontra uma ressalva que deve ser apontada.

O Código de Processo Penal expressa que a incumbência do ônus de provar a alegação a quem a fizer e prevê a possibilidade da produção de provas *ex officio* pelo juiz:

> 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)

O texto do artigo traz aparente contradição com as demais garantais apresentadas, tanto nos princípios do sistema garantias quanto das positivadas no sistema constitucional penal brasileiro. A historicidade do Código de Processo Penal traz resquícios da mentalidade inquisitiva presente quando promulgado como decreto-lei em 1941.

O processo era fundando na busca verdade real, admitindo-se “quaisquer práticas probatórias capazes de sustentar o convencimento do juiz acerca da culpabilidade do suspeito e/ou acusado” (PRADO, 2014, p. 21).

A exposição de motivos do Código de Processo Penal expõe de maneira expressa a intenção de abolir a “injustificável primazia do interesse do indivíduo sobre a tutela social” (CAMPOS, 1941), diminuindo garantias que supostamente favoreciam os criminosos em detrimento da ação repressiva do Estado.

No capítulo dedicado às provas, aponta que o juiz deve ficar subordinado às provas constantes dos autos, porém não deve ser limitado a apurar a verdade material. Não suficiente, aponta a que o juiz não deverá ser inerte da produção de provas, não devendo pronunciar o *in dubio pro reo* enquanto houver ainda fontes de prova a serem exploradas.

A faculdade prevista do juiz de ofício produzir provas nasce, portanto, maculada pela feição inquisitorial que permeava a dogmática processual penal da época. Apesar de prever formalmente a separação entre acusador e julgador, também traz em sua normativa o comprometimento do julgador com uma busca incessante e incondicionada pela verdade que lhe é convicta.

O processo penal não pode ser reduzido a mera cerimônia protocolar, sob pena de violar o devido processo legal. Deve-se caracterizar com a incerteza no início e procurar a certeza como meta. A obrigação de a encontrá-la se posta somente como condição para exercer o juízo condenatório, não como preconiza os princípios que compunham o sustentáculo originário da *lex* processual penal brasileira, exigindo-a em qualquer hipótese.

Tanto o sistema inquisitorial quanto o acusatório tem na prova penal o meio para embasar a verificação dos fatos noticiados como criminosos. Sua diferença se dá no escopo cognitivo delas (PRADO, 2014, p. 20).

Prado (2014, p. 24 e 31) defende que a produção das provas de ofício em si traz feição inquisitorial ao processo penal, na medida que os poderes instrutórios funcionariam como dispositivo apto a preencher lacunas de uma atuação deficiente das partes na instrução, em especial da acusação.

Em um processo penal regulado pela presunção de inocência cabe ao acusador definir o enunciado sobre o fato, lhe incumbindo o ônus de produção da prova e convencimento. De outro lado, caberia ao defensor a busca, seleção, preparação e produção das porções de informações relativas a cada evidência produzida em juízo, enquanto ao juiz cabe controlar a correção dos requisitos de verificabilidade dos fatos e a assegurar a paridade de armas, concretizando o devido processo penal regido pela presunção de inocência (PRADO, 2014, p. 37 e 46).

Badaró (2019), de outro modo, entende ser possível a iniciativa probatória por parte do juiz se coadunar com o princípio acusatório desde que se limite a instruir o procedimento, não investigar.

Quem estiver psicologicamente comprometido com o resultado da busca da verdade tenderá a distorcer sua conclusão, seja pela supervalorização de aspectos que confirmem sua hipótese ou pela ocultação, relativização ou justificativa infundada quando se encontra elementos que neguem o evento (BADARÓ, 2019, p.26)

Carnellutti (2019, p. 47) já alertava a degeneração do processo penal ocasionada ao tornar a descoberta do delito em uma espécie de esporte. Não se pode furtar a necessidade de descoberta do delito, mas atribuir o caráter de meio de divertimento social e consequente onda indiscriminada de procura, conjunturas e informações traz prejuízo ao justo procedimento, sofrendo o julgador com a constante vigilância para que sua convicção confirme alguma construção da opinião pública externa ao procedimento judicial.

Quando o magistrado toma para si uma atividade afeita as partes, corre o risco de perder sua imparcialidade, ou, ao menos, gerar potência dúvidas sobre ela. A determinação de ofício da produção de um meio de prova não requerido pelas partes leva a um prognóstico sobre a expectativa do juiz em obter prova para afastar a dúvida e permitir resolver a demanda com condenação do acusado (BADARÓ, 2019, p. 24).

Instruir não se confunde com investigar, restando o perigo da imparcialidade na busca por fontes de prova. O inquisidor busca apenas a confirmação de um enunciado já previamente escolhido formulado por ele mesmo.

Por outro lado, o juiz que se limita a determinar a produção de meio de prova necessário para incorporar as informações diante da notícia de uma fonte de prova não se compromete com uma convicção prévia norteando uma empreitada investigativa. Nesta hipótese, os enunciados fáticos a serem objetivo de prova já estariam postos e não seria colocado em risco sua posição de imparcialidade (BADARÓ, 2019 p.29).

Cabe ressaltar a diferenciação entre fonte de prova e meio de prova. Fonte é aquilo que fornece a informação sobre os fatos alegados, sejam pessoas ou objetos. Meio de prova são os instrumentos e atividades processuais que se desenvolvem em juízo, pelo qual as fontes de prova introduzem as informações de prova no processo (SANTORO, 2020).

A maioria da doutrina baseada no artigo 156, do CPP, bem como em influência de direito processual civil, afirma que o ônus da prova cabe à acusação quanto à autoria e a materialidade, cabendo ao réu a prova dos fatos impeditivos, modificativos ou extintivos do direito invocado pela acusação. Os riscos da omissão são suportados pelo interessado que não cumpriu seu encargo probatório (GOMES FILHO, 2019).

Nucci (2020, p. 693), por exemplo, atribui o ônus da prova da imputação à acusação, porém indica que o réu pode “chamar a si o interesse de produzir prova, o que ocorre quando alega, em seu benefício, algum fato que propiciará a exclusão da ilicitude ou da culpabilidade”.

Porém, considerando a previsão do artigo 386, inciso VI, do Código de Processo Penal, não se sustenta a posição na qual ao réu se incumbe provar fatos impeditivos, modificativos ou extintivos do direito invocado pela acusação.

Se há previsão de que deverá ser absolvido o réu quando existirem circunstâncias que excluam o crime ou isentem o réu de penal, ou mesmo se houver dúvida sobre sua existência, a incumbência probatória continua da acusação, na

medida que incumbe a defesa gerar dúvida e não certeza sobre tais circunstâncias (DEZEM, 2019).

Gomes Filho (2019, p. 410), também aponta nesse sentido ao afirmar que a disposição da iniciativa das provas não se confunde em estabelecer encargo às partes, muito menos regra de julgamento diversa do *in dubio pro reo*:

> é certo que no processo penal cabe ao juiz esclarecer oficiosamente as questões de um fato, sempre que estiver em situação de dúvida; de outro, não é menos correto que, persistindo a incerteza, só lhe caberá absolver, pela aplicação da regra in dubio pro reo, que é a regra de julgamento que decorre da presunção de inocência. Assim, e à luz das garantias inerentes ao modelo acusatório adotado pela Constituição, a cláusula inicial do art. 156, do CPP deve ser lida como disposição sobre a iniciativa das provas, sem atribuir qualquer encargo às partes – muito menos para a defesa – nem estabelecer uma regra de julgamento diversa do in dubio pro reo.

A sentença favorável à pretensão das partes depende da prática exitosa do ato processual anterior realizado pelo interessado, aproveitando cada chance lhe conferida. Existe uma assunção de riscos na dinâmica processual penal, de modo que mesmo não havendo encargo para a defesa, a não produção de provas pode potencializar uma condenação, portanto, também suportando o réu prejuízo pela sua omissão probatória.

Consequentemente a prova é direito subjetivo do acusado, decorrente do princípio da ampla defesa e do contraditório. A alegação defensiva desprovida de provas poderá ser ineficaz, razão pela qual a atividade probatória defensiva é uma questão de administração de risco, contrapondo o ônus acusatório (MANDARINO, 2016).

Popper (1980, p. 70-71) alerta que é necessário submeter as teorias formuladas a testes severos, visto que se não houver crítica sempre se encontrará aquilo que deseja e não haverá procura pelo que se mostra ameaçador para as teorias que nos agradam.

Se toda hipótese é um enunciado sujeito à verificação, um enunciado acusatório precisa tanto ser confirmada pelas provas que lhe deem suporte quanto resistir aos contrapontos argumentativos apresentados pela defesa (BADARÓ, 2019). A falseabilidade é uma ferramenta de descoberta da verdade, não mero exercício retórico, justamente pela necessidade de se testar a robustez das hipóteses lançadas.

O processo penal já se inicia com uma imputação amparada em um conjunto consistente de elementos de provas, partindo desde o recebimento da denúncia mais próximo da tendência de se confirmar a pretensão acusatória do que a negá-la.

A instrução processual, portanto, servirá para robustecer as provas além da dúvida razoável. Se a regra de julgamento é o *in dubio pro reo*, é na instrução que deve se superar as dúvidas sobre qualquer dos elementos do crime ou da autoria delitiva para ser possível superar o estado inicial de inocência do acusado (BADARÓ, 2019).

Observa-se que eficiência do processo penal não é um necessário contraponto da existência de garantias. A eficiência trata-se de exigir uma constante qualidade na prestação jurisdicional, enquanto as garantias são relacionadas a mitigação do risco inerente do erro judiciário.

A imperfeição do sistema judicial é prevista pelo próprio sistema legal, estabelecendo a responsabilidade de reparar o dano causado por erro judiciário ou prisão indevida na Constituição Federal e a possibilidade revisão criminal no Código de Processo Penal (BRASIL, 1988 e 1941).

Nada impede a conciliação de um sistema eficiente e garantista. Tomando por base a exposição de motivos da Emenda Constitucional 19 (BRASIL, 1998), que instituiu o princípio da eficiência na Administração Pública, eficiência essa correlacionada a gerar mais benefícios, utilizando-se dos recursos disponíveis.

Não há, portanto, contradição em um sistema processual penal ser eficiente e garantista, na medida que maximizar o resultado pretendido com o processo penal em nada tem relação com a minimização das garantais processuais.

A contraposição é da eficácia da pretensão condenatória com as garantias. A aptidão de gerar o resultado pretendido pela acusação é evidentemente diminuída pelas garantias quando se exige um mínimo de robustez ao trazer demandas ao judiciária.

Não se compatibiliza com a ideia de um processo justo permitir qualquer acusação, independente se bem fundamentada ou carente de qualquer justa causa, leve incondicionalmente à acusação. Seria o caso da separação entre acusação e juízo torna-se mera ficção.

De outro modo, a eficiência da acusação é especialmente corroborativa do sistema de garantias. Uma acusação que gere mais resultados pela aptidão de sua pretensão, evitando ao máximo incorrer em nulidades em seu caminho de perseguir a condenação daqueles que comentem injustos penais, expressa o cerne de um procedimento justo e legitimo.

Garantia não equivale a impunidade. A mitigação do risco é relativa ao arbítrio do exercício do poder estatal em cercear a liberdade de um indivíduo, não limitar a punição de infratores de tipos penais.

2. A FUNÇÃO DA PROVA E O OBJETIVO DO PROCESSO PENAL

O processo penal é tanto o instrumento de legitimar a atuação coercitiva do Estado ante o indivíduo delinquente quanto a garantia de resistência contra a arbitrariedade do uso desta força.

Assenta-se que objetivo do procedimento é reconstruir um fato passado para instruir o juízo em sua decisão, definindo Aury Lopes Júnior (2019, p. 341) o processo penal como “um instrumento de retrospecção, de reconstrução aproximativa de um determinado fato histórico”.

Há certo reducionismo na definição pelo seu objetivo. Uma ferramenta pode ser concebida para realizar determinada tarefa, porém ter funções diversas de acordo com aquele que o manipula. No caso do processo, seus agentes têm interesses diversos na resolução do procedimento e isso se reflete diretamente o que os satisfaz como reconstituição daquele fato posto. Ressaltando que a legitimidade de tais pretensões não depende do papel que ocupam, muito menos precisam ser axiologicamente diferentes: tanto o acusador quanto o acusado podem estar buscando justiça dentro do processo, porém cada parte enviesada do que seria justo baseado em sua compreensão sobre o fato.

O andamento do processo não é norteado pela necessidade de conhecimento pleno do fato, mas sim para validar hipóteses apresentadas como o fato. Inicia-se a investigação policial com uma hipótese de ocorrência de crime. Com os elementos colhidos no inquérito policial, o Ministério Público apresenta na denúncia uma nova hipótese sobre o fato. Ao ser denunciado, o réu apresenta em sua defesa uma terceira hipótese.

Desse modo, as versões apresentadas como fato nada mais são do que recortes de um fenômeno maior, delimitadas pelo viés do observador e restringidas pela sua capacidade cognitiva. A conclusão lógica, portanto, é que a justaposição retórica de versões apresentadas pelas partes avança o debate sobre o fato e não a busca da verdade.

A definição supramencionada frisa que a retrospecção se trata de uma reconstrução aproximada do fato, questão de suma importância. A retrospecção do fenômeno originário em sua integridade não somente pressupõe a onisciência e onipotência das partes envolvidas, pressupõe também que seus interesses não se expressam junto com aquilo que alegam.

Limitado a realidade, o procedimento de cognição não há de ser tão exigente de modo a estabelecer critérios irrealizáveis. Se o objetivo é estabelecer a verdade de maneira objetiva, a cognição do juízo de determinado fato por intermédio do processo é falho em sua concepção. É impossível a reprodução perfeita do fenômeno, mas é possível trazer restos de sua existência para o debate, sendo necessário estabelecendo critérios para avaliação destes.

Em nosso caso, o legislador veio a escolher o sistema de livre convencimento motivado, entendimento esse que se extrai da previsão do artigo 155, do Código Penal, combinado com o artigo 93, inciso IX, da Constituição Federal (BRASIL, 1941 e 1988). Retirando-se da equação os fatos axiomáticos, notórios e as presunções legais absolutas, cabe a cada parte comprovar sua alegação, induzindo o juízo a compreender a situação sob o viés de seu recorte da realidade.

O instituto da prova, portanto, presta-se a estabelecer sustentáculo às alegações lançadas, confirmando-as, afastando-as ou até mesmo trazendo incerteza a hipótese articulada. Ante o princípio do contraditório, pressupõem-se inexistirem provas absolutas, sendo sempre possível argumentar em senso contrário aquilo apresentado. A possibilidade de argumentar e a capacidade do argumento convencer alguém, por outro lado, não são necessariamente grandezas correlatas. O direito de ser ouvido não se confunde com o mérito de ter sua pretensão reconhecida, porém implica no enfrentamento do contra-argumento pelo juízo.

Se a prova sustenta os argumentos apresentados, a retrospecção é um elemento do processo, não seu objetivo. A prova fundamenta a dinâmica processual posta, justificando e influenciando o juízo a decidir. O meio estabelecido para alcançar a retrospecção é o sistema probatório, mas o objetivo do processo é a decisão do juiz, sendo lá onde se expressa o objeto da prova e o resultado da persuasão (PRADO, 2014, p. 36).

O procedimento realizado a alcançar a decisão não pode ser mera formalidade a legitimar a decisão exortada. Somente o processo que parte da incerteza e se encaminha para produção da certeza realiza o ideal do devido processo penal (PRADO, 2014, p. 17).

Não resta espaço em uma constituição democrática para razão absoluta do Estado. Os juízes criminais da tradição anterior a redemocratização instituíam a verdade oficial (PRADO, 2014, p. 32).

O juiz é livre para formar sua convicção desde que seja fundamentada em provas, ou pelo menos não seja fundamentada exclusivamente em elementos informativos pré-processuais, ressalvando as provas cautelares, não repetíveis e antecipadas. Porém, mesmo que seu convencimento seja livre, há previsão expressa da inadmissibilidade das provas ilícitas, impondo-se assim um controle do que é conhecível pelo juízo como fundamento para sua convicção.

O controle da validade da prova é técnico, devendo obedecer aos critérios legais para sua produção, corroborando em preservar sua integridade e confiabilidade, sendo sua qualidade e legalidade desafiadas por argumentos técnicos.

Assim, a metodológica da produção das provas não se confunde com convicção na decisão judicial. É necessário garantir validade e autenticidade das informações prestadas pelas provas apresentadas, de modo a afastar incertezas e permitir a convicção do julgador livre de vícios.

A expressão da convicção, livre desde que fundamentada, é resultado do convencimento efetuado pelos argumentos e provas lançadas ao julgador. Como defende Aury Lopes Júnior: “A decisão judicial não é a revelação da verdade [...], mas um ato de convencimento formado em contraditório e a partir do respeito às regras do devido processo” (LOPES JÚNIOR, 2019, p. 376).

A oportunidade de oferecer contraditório no processo é essencial para sua validade. A contribuição das partes cujos efeitos da decisão irão recair lhes concede o poder de influenciar o julgamento final, de mesmo modo que legitima o resultado com sua participação. Nas palavras de Antônio Magalhães Gomes Filho (2019, p. 405-406):

> Ao estabelecer que o juiz formará o seu convencimento pela livre apreciação da prova produzida em contraditório judicial e excluindo, ao mesmo tempo, que possa utilizar exclusivamente elementos informativos colhidos na investigação, o legislador sublinhou que a observância do contraditório é verdadeira condição de existência da prova.
>
> De fato, só podem ser considerados como provas, no sentido jurídico-processual os dados de conhecimento introduzidos no processo na presença do juiz e com participação das partes, em contraditório. Daí porque somente tais elementos podem servir à formulação do juízo de certeza próprio da sentença, ao passo que as informações colhidas na fase de investigação – que podem, quando muito, levar a um juízo de probabilidade, idôneo para fundamentar a acusação ou adoção de medidas cautelares –, não podem ser utilizadas, sem amparo em verdadeiras provas, para condenar.

No caso das provas antecipadas, não repetíveis ou cautelares, precisamente pela natureza excepcional de urgência ou impossibilidade, necessitam de providencias justificadamente apressadas, adiando o contraditório. Com o contraditório diferido, já em fase processual, são analisados tanto a qualidade da prova quanto a legalidade e condições de sua produção fora do contraditório judicial.

Ainda, até a prova emprestada, considerada aquela produzida em outro processo, só pode ser utilizada se as partes forem as mesmas em ambos, além de que se tenha realizado o contraditório no procedimento original.

A convicção expressa na sentença pelo juízo concretiza o valor de cada prova referente ao fato em lide. O juiz quem decide se foram comprovados ou não as questões fáticas alegadas, sendo um típico ambiente de conhecimento incerto. Toda prova trazida ao juízo trabalha a qualidade da retrospecção, mas não se pode garantir uma decisão favorável na medida que o convencimento é uma questão de probabilidade e não de certeza (BADARÓ, 2019, p. 20).

O processo resulta em uma decisão absolutória ou condenatória na esfera penal, sendo o escopo da atividade probatória os limites da decisão possível. Mesmo que seja impossível reproduzir a realidade, a busca da verdade torna a decisão mais justa.

Tomando como parâmetro o artigo 386 do Código de Processo Penal (BRASIL, 1941), a decisão absolutória se encontra no espetro da incerteza (incisos II "não haver prova da existência do fato"; V "não existir prova de ter o réu concorrido para a infração penal" e VII "não existir prova suficiente para a condenação") e da certeza (incisos I "estar provada a inexistência do fato"; III "não constituir o fato infração penal"; IV "estar provado que o réu não concorreu para a infração penal" e VI "existirem circunstâncias que excluam o crime ou isentem o réu de pena"). A condenação, de outro modo, se encontra somente no campo da certeza.

Certeza implica reconhecer algo como verdade. Se é impossível reproduzir a realidade e a verdade objetiva não se revela por intermédio do processo penal, trata-se de uma convicção sobre a realidade por parte do julgador, que lastreia decisão na percepção sobre os fatos que lhe foi possível atingir no procedimento. A verdade reconhecida, portanto, é uma construção processual (BADARÓ, 2019, p. 20).

A impossibilidade de reconhecer a verdade em sua totalidade não tem como consequência a conclusão de inexistir verdade em absoluto. O fenômeno existe ou não existe, o que é relativo é a possibilidade de confirmar ou não sua existência no processo penal. O enunciado apresentado ao juízo pode ser potencialmente verdadeiro ou não, mas o *thema probandum*, o fato sobre o qual se versa a discussão, é identificado em absoluto como verdade ou não, sem espaço para relativização (BADARÓ, 2019, p. 88-91).

A prova tem a função de retrospeção, trazer resquícios do passado para uma análise presente. Sujeita ao controle de sua validade e ao contraditório, serve de fundamento para as alegações das partes e são elementos de convicção do juízo sobre um fato.

Logo, o processo penal tem como objetivo o provocar o juízo a decidir sobre uma pretensão acusatória, confirmando-a ou rejeitando-a conforme o desenvolvimento do processo afeta seu convencimento.

2.1 – Construção da verdade

Se a cognição processual é meio para fundamentar a decisão do juízo, não é exercida pela simples curiosidade. A retrospeção aventada é articulada pelas partes em contraditório em busca de uma decisão favorável à sua respectiva pretensão.

Tais articulações se apresentam como narrativas processuais, construções interpretativas dos eventos. São apresentadas possibilidades, dando forma coerente aos resquícios do passado disponibilizados. (TARUFFO, 2016, p. 54)

As narrativas também abrem caminho para a imprecisão, variabilidade e manipulações na reconstrução dos fatos. Os sujeitos elaboram suas narrativas conforme seu ponto de vista, interesses e limitações, situados em um momento e determinado contexto (TARUFFO, 2016, p. 55).

A complexidade da relação processual é composta por várias histórias construídas e contadas por sujeitos diferentes, de modos diferentes e de pontos de vista diferentes. Frequentemente a cognição judicial fica vulnerável ao erro, incompletude, manipulação e imprecisão das reconstruções do fato que se apresentam (TARUFFO, 2016, p. 55).

Em um caso judiciário real, se pressupõem que os enunciados deveriam ser verdadeiros. O contexto exige a descrição da realidade, mas a qualidade da narrativa não se correlaciona com a verdade, mas sim com a verossimilhança. É persuasiva uma narrativa que apresente coerência, confiabilidade, trivialidade e familiaridade, não necessariamente aquela que mais se aproxima da realidade (TARUFFO, 2016).

Razão pela qual os aspectos fáticos das narrativas processuais são objeto de prova, verdadeiros ou falsos. Os enunciados de direito, os aspectos jurídicos, são objetos de valoração baseada em escolha, interpretação, argumentação e de justificação. (TARUFFO, 2016, p. 60)

O aspecto jurídico é normativo. A articulação, seja hermenêutica ou puramente argumentativa, se revela a partir da performance das partes na construção narrativa. Ela é objeto de escolha, interpretação, argumentação e justificativa (TARUFFO, 2016, p. 61)

Isto posto, ainda que a relevância da prova seja delimitada pelos fatos principais controvertidos, os aspectos jurídicos controlam sua validade e admissibilidade. Consequentemente, o escopo cognitivo da verdade é axiomático.

De qualquer modo, a realidade deve ser o critério de verdade, há necessidade de que haja uma relação de correspondência entre o enunciado fático e o fenômeno

real objeto do julgamento. A lei atribui consequências jurídicas à realidade, não a uma narrativa coerente.

É na decisão que o objeto da prova se torna visível. A verificação da pretensão acusatória pelo Poder Judiciário é relativa ao fato atribuído ao imputado. Parte-se da justa causa, a probabilidade da ocorrência, para buscar a construção da certeza do fato e autoria, tendo como consequência a condenação, se obter êxito em provar.

Se exige melhor prova para ultrapassar a presunção de inocência, sendo a verdade no processo penal ordenada por meio de requisitos de verificação dos fatos da causa, com capacidade de limitar a discricionariedade do julgador (PRADO, 2014, p. 39)

As regras dirigidas à paridade de armas são evocadas como premissa de um julgamento justo, compensando a diferença de forças entre as partes por obrigações processuais limitadoras da intervenção penal (PRADO, 2014, p. 51 e 52).

Os critérios de verificação da verdade são relacionados a distribuição do ônus da prova. O requisito para construção da certeza é diretamente relacionado ao encargo de provar o alegado.

A verificação da jurisdição não se resume ao exame da justa causa, também abrangendo a legalidade da atividade preparatória. Se realiza o crivo sobre a estrita legalidade da obtenção e preservação dos meios de prova em condição de serem consultadas oportunamente pelas partes (PRADO, 2014, p. 55).

Se instaura um nexo funcional no campo processual equivalente ao que se verifica no direito material, prevendo proibições destinadas aos agentes públicos responsáveis pela persecução criminal (DEZEM, 2019).

A possibilidade de uma decisão arbitrária depende unicamente da possibilidade de decidir, razão pela qual deverá ser articulada com a decisão política que a lei expressa, dialogando racionalmente com o expresso no texto legal. A sujeição do juiz exclusivamente à lei, portanto, reveste-se de enunciado prescritivo, não mera descrição (PRADO,2014, p. 63-65).

A atividade probatória é intimamente ligada a participação humana. É produzida com a participação das partes, testemunhas, peritos, assistentes técnicos e vítimas. Se destina ao juiz, figura igualmente humana, cujo fundamento da decisão consistirá no grau de persuasão depreendido da racionalidade das provas apresentadas (MANDARINO, 2016).

No ambiente processual, a divisão de conhecimento entre as partes, em posições antagônicas, nem sempre assegurará que o saber produzido seja próximo do ideal: “as partes normalmente selecionam fatos que lhes favorecem e omitem os que potencialmente possem lhes prejudicar” (BADARÓ, 2019, p. 34).

Ao final do procedimento, o juiz estabelece qual das diversas narrativas dos fatos é melhor, escolhendo reativamente uma das versões apresentadas ou construindo uma original se insatisfeito com aquelas lhe apresentadas pelas partes (GOMES FILHO, 2019).

Segundo Taruffo (2016), a narrativa apresentada na decisão final se reveste de três características relevantes: constitui uma série de enunciados descrevendo fatos; é neutra, anticompetitiva, tendo função de confirmar de modo objetivo determinados fatos, visto que seu compromisso seria com uma decisão justa e precisa, não com as partes; e pretende verdadeira por estar baseada naquilo que entende provado nos autos.

2.2 Limites epistemológicos

As regras de exclusão visam um resultado probatório de melhor qualidade, embora restrinjam o escopo de elementos valoráveis e potencialmente persuasivos. Limita-se o ingresso preventivo de elementos de prova que possam gerar uma inexata reconstrução dos fatos (BADARÓ, 2019).

O conjunto de provas em um processo penal não resulta na verdade judicial. O condicionamento da realidade processual se dá nos limites probatórios em prol do *status libertatis* do acusado, assegurando o respeito ao devido processo legal e a dignidade humana. A pretensão acusatória deve ser proposta sem causar constrangimentos à dignidade do acusado e as formalidades processuais (MANDARINO, 2016).

Até porque, o desconhecimento da lei é inescusável, como prevê o artigo 21 do Código Penal (BRASIL, 1940), não podendo o Estado ignorar a lei em benefício da sua discricionariedade.

Em sentindo contrário, há posição de que as regras de exclusão não são tão relevantes, na medida que não são as principais causas de condenações injustas. Os reais responsáveis pelas condenações errôneas são a má performance da defesa e acusação, além da identificação incorreta por testemunhas oculares e falsas confissões, ou, ainda, a visão de túnel da investigação, sendo pouco relevante o erro na interpretação da prova (HADJIMATHEU, 2020, p. 32).

Por visão de túnel da investigação entende-se o viés que toma a investigação ao se concentrar em um suspeito, trabalhando no sentido de criar um caso de condenação, não na busca da verdade. O investigador se engaja no resultado da investigação, ocasionando em ignorar ou suprimir provas que apontem em sentido contrário à sua convicção de que o investigado é culpado (HADJIMATHEU, 2020, p. 32).

Ocorre que as regras de exclusão probatória não se resumem a intuir assertividade nos julgamentos. Considerando que as garantias resguardam o indivíduo da ingerência estatal em sua vida privada, não se sustenta renegar relevância às regras de exclusão a tal critério.

Assertividade das decisões judiciais é algo desejável, porém não a qualquer custo, sob pena de retornar à já abordada mentalidade inquisitiva.

O princípio da liberdade probatória rege o processo penal, havendo limites em seu exercício. Há um rol de provas previstos no Código de Processo Penal, todavia,

não fica a atividade probatória limitada somente aquelas previstas em lei. Observada a restrição quanto ao estado das pessoas do parágrafo único do artigo 155, do Código de Processo Penal (BRASIL, 1941), não há vedação a utilização de provas não previstas em lei, desde que subordinadas aos limites legais e constitucionais. Assim, encontramos provas típicas e atípicas, diferenciadas pela previsão ou não de procedimento para sua produção (FERNANDES, 2011, p. 15).

A diferença na obtenção de provas típicas e atípicas é de fundamental importância para sua licitude. A prova típica deve obedecer ao procedimento especificamente previsto para ela, sob pena não se legitimar sua validade. A atípica tem inicialmente o crivo da tipicidade, ou seja, de que aquela prova apresentada não é uma variação de prova típica apresentada como atípica para circundar seus requisitos legais, seguido do crivo constitucional legal, em conformidade com as garantias constitucionais e processuais atinentes à prova penal.

O tratamento das provas ilícitas no processo penal é claro, ante a previsão do artigo 157, do Código de Processo Penal (BRASIL, 1941), são inadmissíveis e devem ser desentranhadas do processo, inclusive as aquelas derivadas das ilícitas. Tal previsão tem fulcro constitucional, considerando o disposto no artigo 5º, inciso LVI, da Constituição Federal: “são inadmissíveis, no processo, as provas obtidas por meios ilícitos” (BRASIL, 1988).

A doutrina diferencia provas ilegítimas e ilícitas. É ilegítima quando produzida em contrariedade ao direito processual, tendo como consequência a nulidade e logo deve ser renovada ou retificada, incluindo os atos consequentes, conforme a previsão do artigo 573, do Código de Processo Penal. A ilícita, por outro lado, contraria direito material em sua obtenção, de modo que não deveria ingressar no processo, sendo inadmissível, nos termos do já referido artigo 157, do Código de Processo Penal (BRASIL, 1941).

Ainda, há vedação as provas ilícitas por derivação. O Código adota a teoria dos frutos da árvore envenenada no tratamento das provas derivadas das provas ilícitas, entendendo que uma vez violada a legalidade da obtenção da prova, toda atividade probatória consequente macula-se, de maneira que também não pode ser admitida. A vedação vem no sentido de reprimir a obtenção de provas por via ilícita, pois ilógico seria admitir a validade dos reflexos de um ato ilícito inadmissível.

Há ressalva quanto a admissibilidade de provas derivadas da ilícita quando não evidente o nexo de causalidade ou elas puderem ser obtidas por uma fonte independente das primeiras.

O conceito legal de fonte independente encontra previsão no parágrafo 2º, do artigo 157, do Código de Processo Penal: “Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova.” (BRASIL, 1941). Assim, pela definição apresentada, entende-se que o legislador teria adotado a exceção da descoberta inevitável, como defende Guilherme Madeira Dezem (2019, p. 598):

> Tendo em vista a redação dada pelo legislador, nos parece que não há que se falar em positivação da teoria da fonte independente. Para a teoria da fonte independente há necessidade de que, concretamente, haja presença de ambos os meios de prova [...]. Parte-se, para exceção da fonte hipotética independente, da análise abstrata do caso, sem a necessidade de que, concretamente, haja a presença da fonte de prova lícita [...] Deve-se analisar se, naquele caso concreto, haveria inevitabilidade da descoberta da prova. Está análise deve ser feita considerando-se a linha investigativa desenvolvida naquela específica investigação e não por meio de esquemas mentais abstratos e genéricos.

O advento da Lei 13.964/19 formalizou no Código de Processo Penal a cadeia de custódia, sendo definida no *caput* do artigo 158-A do referido *códex* como o “conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte”, delimitando vestígio em seu § 3º como “todo objeto ou material bruto, visível ou latente, constatado ou recolhido que se relaciona à infração penal” (BRASIL, 1941).

O artigo 158-B dispõem sobre as etapas de rastreamento dos vestígios, delimitando-as em reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte.

Os artigos 158-C a 158-F vêm determinar a forma para o cumprimento da cadeia de custódia de acordo com as etapas predefinidas, prevendo obrigações mínimas para conduzir o procedimento ante os vestígios.

A preocupação com a aplicação da cadeia de custódia das provas visa assegurar a confiabilidade e integridade dos elementos probatórios. A sistematização de procedimentos e responsabilidades aos sujeitos que entrem em contato com as

provas no âmbito da investigação e processo penal traz um arcabouço para auferir condições mínimas de legitimidade daqueles elementos e, consequentemente, garantia de contraditório adequado quando foram apresentadas.

A importância da cadeia de custódia e consequente validade da prova já era um instituto reconhecido pela doutrina e jurisprudência brasileira.

Geraldo Prado explica existir um sistema de controle epistêmico da atividade probatória que assegura a autenticidade de determinados elementos probatórios, estabelecendo de maneira objetiva um procedimento que garanta e acredite a prova independente da problemática em torno do elemento subjetivo do agente que manusear a prova.

Apresenta como exigência para validade das provas neste controle a Sumidade, que compreende na garantia de que aquela prova valorada é exatamente e integralmente aquela que foi colhida, e a Desconfiança, consistindo na exigência de que a prova deve ser legitimada através de um procedimento que demonstre que tais objetos correspondem ao que a parte alega ser (PRADO, 2014, p. 16-17).

3. PROVA DIGITAL

As inovações tecnológicas, como o registro audiovisual amplamente acessível a população ou a proliferação de câmeras de vigilância em empreendimentos e residências, parecem assegurar o acesso à realidade como objeto autônomo do conhecimento, como ter acesso à verdade como ela é, por se apresentar desvinculada de narrativas.

Este ângulo equivocadamente retoma a mentalidade de que o contraditório judicial seria um veículo de contaminação da verdade para assegurar a impunidade dos acusados. Atribui-se a imagem e som correspondência de espelho fiel da realidade, sem levar em conta o meio que abriga tais expressões, o arquivo digital, criando um consenso ilusório de infalibilidade e correção (PRADO, 2014, p. 69 e 73).

O armazenamento de informações em meio digital possibilita sim meios mais robustos de reproduzir elementos fáticos documentados, mas não retira sua qualidade de prova sujeita à apreciação. Mesmo imagens fidedignas são mera representação digital do fato e não o fenômeno originário, podendo sofrer distorções invisíveis aos mais incautos.

Thamay e Tamer (2020, p. 32) escolheram conceituar a prova digital como a demonstração de fatos ocorridos em meio digital ou a demonstração por meio digital de fatos não necessariamente ocorridos no meio.

Complementando tal conceituação, entende-se que a prova digital é a prova cuja informação apresentada é preservada em meio digital, independentemente do fato demonstrado pela informação ter ocorrido em meio físico ou digital.

De uma maneira simples e abstrata, um arquivo digital é o armazenamento de um segmento ou bloco de informação disponível a um programa de computador (FEDERAL AGENCIES DIGITAL GUIDELINES INICIATIVES, 2020). Na introdução foi utilizada uma conceituação mais pragmática, de que os arquivos digitais fornecem informações através do processamento de dados neles contidos (MASSON, 2017, p. 672).

Nossa interação convencional com tecnologia informática é feita por meio de sistemas operacionais comerciais. Tais sistemas simplificam a parte técnica de utilizar um computador ou celular, garantindo a acessibilidade a pessoas leigas, mas de mesmo modo escondendo boa parte dos processos que ocorrem para que cada ação seja realizada. Assim, a referida conceituação é suficiente e eficiente para expor a dinâmica posta e problematizá-la no âmbito probatório.

Porém, bem como o sistema operacional, o véu da simplificação nos priva de conhecer a integralidade do processo realizado, deturpando a percepção sobre a complexidade e/ou precisão atingida em proporção equivocada à facilidade de acesso e uso de determinado programa de computador ou arquivo.

Considerando a questão do controle de validade e efetivo exercício do contraditório, volta-se à literatura informática para fundamentar a descrição do que seria o procedimento de preservação digital de informações de modo mais assertivo. Para tanto, neste momento prestigia-se a terminologia técnica da informática em detrimento da simplificação instrumental voltada à prática jurídica.

Posto isso, em termos técnicos, o arquivo é um dos componentes de uma informação sujeita a preservação em meio digital. Para descrever o procedimento de preservação de informação em meio digital, será utilizado como inspiração um modelo de preservação de metadados digitais, ou seja, preservação dos dados sobre dados alocados em meios digitais.

O PREMIS *Data Dictionary* (2015) é um documento elaborado com a finalidade de estabelecer um padrão internacional de estruturação de sistemas para a preservação de metadados relacionados ao processo de preservação digital de informações, propondo um modelo de implementação baseado 4 entidades principais: objeto, evento, agente e declaração de direitos.

Objeto é uma unidade discriminada de informação sujeita a preservação digital.

A informação que propriamente se pretende preservar é denominada entidade intelectual, podendo ser um vídeo, um livro ou até um programa de computador. Entidades intelectuais podem incluir outras entidades intelectuais. Determinadas entidades intelectuais são denominadas ambiente. O ambiente é a tecnologia que suporta o objeto digital em de alguma maneira. A tecnologia pode ser um programa de computador (*software*) ou o próprio computador (*hardware*), enquanto o suporte pode ser tanto em sua criação ou como meio de acesso à informação.

A informação é entregue através de uma representação, que é um arquivo ou conjunto de arquivos necessários para reprodução daquela informação. Uma entidade intelectual pode ter mais de uma representação, digital ou não.

A título de exemplo, um livro pode ser representado em um arquivo PDF em sua integralidade, por vários arquivos de imagem JPEG sequenciais para cada página ou, ainda, pode ser impressa em papel para acesso em meio físico.

Um arquivo é uma sequência de dados nomeada e ordenada de modo a ser reconhecida por um sistema operacional. Cada arquivo tem um formato (como os mencionados PDF e JPEG), permissões de acesso e características do sistema de arquivos como tamanho e data de modificação.

Evento é uma ação que envolve ou afeta ao menos um objeto ou agente. O registro de eventos é a garantia de autenticidade da informação preservada. A robustez dos registros é diretamente ligada ao sistema utilizado para interagir com o a informação, determinada pelos interesses e objetivos quando da estruturação do sistema.

Agente é a pessoa, organização ou ambiente associado aos eventos na vida do objeto ou com os direitos fixados ao objeto. Um agente interage ou se associa aos eventos e/ou direitos diretamente ou através de outros agentes.

A declaração de direitos é afirmação de direitos ou permissões pertinentes ao objeto ou agente. Isso inclui o direito de acessar o arquivo, extrair dele uma representação, modificá-lo ou ainda transferi-lo a outro local.

A título de exemplo, atente-se ao acesso de determinado documento dentro de um servidor de determinada organização por determinado funcionário.

A organização tem permissão de acesso ao documento. O funcionário é integrante da organização. O funcionário (agente) utiliza um computador (agente) com um programa de leitura de PDF (agente) para acessar (evento) um documento digitalizado (objeto), lhe sendo permitido acessar as informações preservadas do documento ante sua associação de integrante da organização com direito à acesso (declaração de direitos).

De modo pragmático, a conduta do funcionário se resumiu a pequenos cliques com o *mouse* do computador. Porém, o acesso e preservação daquelas informações depende de interações ocultas ignoradas pelo usuário.

A complexidade de um sistema é inversamente proporcional à sua segurança. Quanto maior o número de interações entre entidades, maior o risco que alguma delas apresente uma vulnerabilidade (ALIMONTI, 2019, p. 52).

Se situações corriqueiras são sujeitas a uma complexa gama de interações ocultas, escondidas pela simplicidade de uso das ferramentas tecnológicas, pretensa infalibilidade atribuída aos meios de prova digitais só subsiste na ignorância técnica do funcionamento da tecnologia empregada.

Nos termos dos artigos 158 e 159, do Código de Processo Penal (BRASIL, 1941), toda vez que uma infração deixar vestígios será indispensável o exame de corpo de delito, realizado por perito oficial. Segundo o artigo 158-A, §3º, da mesma lei, “vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal”.

A necessidade de utilizar conhecimentos especializados traz fundamental importância da perícia enquanto meio de prova. O perito, portanto, fica responsável em traduzir a invisível complexidade técnica para os agentes processuais. A representação *prima face* das informações apresentadas pode confundir as partes, pela verossimilhança atribuída aos registros audiovisuais pelo brocardo popular “uma imagem vale mais que mil palavras”.

Ocorre que se tratando de armazenamento digital, qualquer representação audiovisual pode ser reduzida a caracteres, de certo modo esvaziando o sentido da máxima aludida. A prova cientifica possibilita vencer a obscuridade, mas também traz problemática se revestida de autoridade absoluta sobre o objeto de prova.

Não se pode furtar do devido enfrentamento da informação acostada no laudo pericial, suas conclusões também são resultado de probabilidade, da busca da verdade e não da absoluta verdade.

“O mito da infalibilidade das provas cientificas oculta o risco do juiz achar que não é necessário justificar sua decisão” (BUSTAMENTE, 2020, p. 278). A probabilidade de uma hipótese implica ser possível demonstrá-la pelas provas disponíveis e excluir as hipóteses alternativas, decorrendo o grau de confirmação pela qualidade dessas inferências, podendo aumentar ou diminuir de acordo com o grau segurança acreditado aos métodos utilizados pelo profissional técnico.

O risco do juiz e as partes se tonarem destinatários passivos informações incompreensíveis, cuja idoneidade não pode ser verificada é combatida pela possibilidade de verificação dos conhecimentos utilizados, a consciência sobre a potencialidade de equívocos e a relevância especifica aos fatos da causa.

O artigo 182 do Código de Processo Penal (BRASIL, 1941) impõem que o juiz não fica adstrito ao resultado do laudo, assim, todas as provas tornam-se relativas frente ao seu próprio convencimento

Se cabe ao juiz a última palavra sobre o resultado da perícia, falta de domínio do assunto esvazia a efetividade deste juízo. A falta de elementos para que ele possa

exercer algum tipo de controle sobre o conteúdo do laudo pode levar a conclusões distorcidas (GOMES FILHO, 2019, p. 419).

As teorias nascem para serem superadas, portanto todo saber é datado, relativo ao avanço científico de determinado recorte temporal (LOPES JÚNIOR, 2019, p. 424). A prova cientifica é tão relevante quanto a qualidade das informações que ela presta, não podendo elencá-la a valoração absoluta, não isentando o juízo de motivar suas decisões, pautando-se no conteúdo e não na mera existência da prova.

É necessário distinguir ciência válida da inválida, eliminando ruídos de informações inconsistentes. A consistência e validade é provada pela adoção de procedimentos adequados e validados pela comunidade cientifica com evidências empíricas de sua confiabilidade, articulando de modo racional e não pela simples remissão teórica. “Não é porque existem livros de extraterrestres (na *Amazon* são mais de 6 mil títulos) que se prova a existência de vida fora da terra” (ROSA, 2021, p. 408).

As informações armazenadas em meio digital, os vestígios digitais, apresentam características especificas que se destacam da contraparte analógica/convencional: imaterialidade, volatilidade, fragilidade e dispersão.

Imaterial em razão de ser composto por dados alocados.

Volátil em decorrência da facilidade em desaparecer como consequência de uma ação do usuário.

Frágil ante sua vulnerabilidade a manipulação, intencional ou não, pelo próprio usuário ou ambiente em que se acessa à informação.

Disperso porque existe a possibilidade de partes de uma mesma prova digital estar alocada em locais diferentes dentro do mesmo sistema informático ou mesmo em diversos locais físicos (NERES, 2021, p. 347-348).

Tais especificidades são prejudiciais na busca de atribuir à prova digital confiabilidade e integridade sob os critérios de sumidade e desconfiança elencados.

No âmbito puramente técnico, a norma ABNT/ISO 27037:2013 traz diretrizes padronizadas para identificação, coleta, aquisição e preservação de vestígio digital.

A identificação consiste no reconhecimento de potencial vestígio digital, elencando inclusive prioridade para a coleta baseada na volatilidade da evidência.

Na coleta são removidas as evidências digitais em potencial de sua localização original para um ambiente controlado. O procedimento utilizado depende

do estado do ativo, na medida que o acesso, relevância e como as informações se apresentam, são diferentes em razão do estado.

Por exemplo, um computador ligado e logado pelo usuário daria acesso ao perito aos arquivos armazenados sem maiores resistências, torna relevante preservar o ambiente de *software* ativo no momento da diligência enquanto diretamente relacionado às informações representadas diretamente no aparelho informático.

Se estivesse desligado, maior relevância seria coletar as informações armazenadas no disco rígido do computador sem ativá-lo, visto que garantiria a integridade das informações sem interferência do perito.

A aquisição, etapa terceira, é o momento em que se produz cópia da evidência digital e se documenta o procedimento realizado para acessá-la, registrando os motivos de cada decisão relacionada a situação dos ativos, de modo a permitir a reprodução e verificação dos métodos posteriormente por profissional capacitado e independente.

A última etapa consiste na preservação da evidência digital, protegendo sua integridade. A norma prevê que o compromisso com a preservação inicia desde a identificação potencial do vestígio digital, levando em conta justamente a fragilidade e volatilidade da prova em potencial (NERES, 2021, p. 352/353).

O procedimento operacional padrão destinado aos peritos criminais na área de informática forense (SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA, 2013, p. 89) aponta que o laudo pericial sobre mídias digitais deve observar os seguintes tópicos:

> Informar se os exames foram realizados diretamente sobre a mídia original ou sobre a cópia; no primeiro caso, deve-se explicar quais foram os motivos e os procedimentos utilizados para garantir a integridade dos dados.
> Relatar, se for o caso, que procedimentos de recuperação de dados apagados ou corrompidos (dentre outros) foram utilizados, e que os exames foram feitos não apenas sobre os arquivos diretamente acessíveis, mas também sobre aqueles apagados (fragmentados, corrompidos, etc.) e passíveis de recuperação.
> Descrever os exames de forma proporcional à sua complexidade, evitando-se assim descrições extensas e complexas para laudos simples, e vice-versa.
> Especificar os softwares utilizados durante os exames somente quando essencial para a compreensão dos procedimentos adotados ou para futuras verificações dos resultados.
> Descrever as técnicas periciais propriamente ditas, e não os detalhes da utilização dos aplicativos forenses.
> Para o caso de existência de mídia anexa ao laudo, explicar que os arquivos ali gravados foram submetidos a uma “função de *hash*” para fins de garantia de integridade.
> Mencionar eventuais alterações (físicas ou lógicas) promovidas no material examinado

Há evidente preocupação em relatar o procedimento, porém resume a garantia de integridade da informação apresentada com o laudo por meio de função *hash*, que consiste em um algoritmo que transforma qualquer informação em um dado de largura fixa, condensada em 20 bytes independentemente do tamanho do original (MENKE, 2019, p. 134).

O confronto de função de *hash* permite identificar alterações no conteúdo da mensagem, mas não garante a integridade original da informação vestigial. A função de *hash* é um resumo do conteúdo original, mas a integridade não se resume a conferência de não alteração do resumo.

Alterações anteriores à submissão do vestígio à função não poderiam ser confrontadas. A integridade a qual o documento se refere, portanto, é da mídia que acompanha o laudo, não do vestígio periciado.

Baseando-se nas boas práticas da *Internet Engineering Task Force* (IETF) (NETWORK WORKING GROUP, 2002) para coleta e arquivamento de vestígio digital relevante, o vestígio digital deve ser admissível, autêntico, completo, confiável e acreditável.

Admissível por dever seguir as regras legais para sua admissibilidade jurídica. Autêntica na medida que deve ser possível ligar o vestígio material ao fato. Entende ser completa pois deve apresentar toda informação relevante, não só aquilo que é interessante a uma das partes. Confiável ante a necessidade de extirpar quaisquer dúvidas sobre sua autenticidade e veracidade na sua coleta e manipulação. Acreditável em razão de não ser suficiente a garantia de sua confiabilidade, ela deve ser entendida e compreendida como tal em juízo.

Também apontam quais informações seriam necessárias para que se atinjam tais características, indicando a necessidade de manter a cadeia de custódia. De modo cristalino deve descrever como o vestígio foi encontrado, como ele foi manuseado e tudo que aconteceu com ele, documentando onde, quando e por quem foi descoberto e coletado, bem como manuseado e examinado.

Indica também a necessidade de armazenar em mídia comum para ampla acessibilidade em formato que permita ser só possível a leitura, evitando a manipulação das cópias, ao mesmo tempo que deva ser possível detectar acesso desautorizado.

Quanto as ferramentas utilizadas, elenca que devem ser capazes de examinar os processos de um dispositivo informático, o estado do sistema operacional, permitir

a cópia integral dos dados, que gerem assinaturas e a checagem de integridade do armazenamento e transferência dos dados, que permitam gerar uma representação dados e examiná-los, bem como funcionarem com a coleta automatizada dos vestígios, eliminando interferência humana no processo.

Tais práticas levam em conta que o armazenamento de informações eletrônicas é realizado pelos mais diversos dispositivos, formatos e idiomas, podendo comprometer a qualidade dos registros e consequentemente a análise técnica, gerando incompatibilidade com as ferramentas de análise forense disponíveis (NASCIMENTO, 2020, p. 121).

No *Habeas Corpus 160.662*-RJ (BRASIL, 2014), o Superior Tribunal de Justiça decidiu pela anulação de provas produzidas em interceptação telefônica e telemática que, apesar de legalmente deferidas no caso, foram parcialmente extraviadas na Polícia e não foram disponibilizadas da forma como captadas.

Entendendo decorrer da garantia da ampla defesa o direito do acusado à disponibilização da integralidade de mídia e que a prova produzida durante a interceptação não serve apenas aos interesses do órgão acusador, foi concedida a ordem, de ofício, anulando as provas produzidas nas interceptações e aquelas ilícitas por derivação.

Agora com a previsão legal da cadeia de custódia esse controle ganha um sustentáculo para oposição do referido controle epistêmico, porém, em leitura atenta aos dispositivos referentes a ela no Código de Processo Penal, percebe-se que a lei falha a se manter atual definindo como vestígio objetos e materiais brutos, não abarcando, em primeiro momento, aquelas evidências contidas em arquivos digitais.

Porém, entendendo os arquivos digitais como um conjunto de símbolos codificados que quando processados nos fornecem informações, tais códigos seguem armazenados no *hardware* das máquinas, sejam computadores pessoais ou em servidores de empresas.

Utilizando de exemplo o funcionamento disco rígido, que grava a informação codificada de modo binário, alterando com um imã de forma mecânica fragmentos do disco entre ativados e desativados (os ‘0’s e ‘1’ do código), as alterações em arquivos digitais tem reflexo no mundo físico, ainda que não seja imediatamente perceptível.

Assim, a legislação deve abarcar as provas digitais e, consequentemente, deverão ser estabelecidos procedimentos adequados para resguardar a integridade

tanto do objeto de armazenamento quanto o arquivo em si, ou até mesmo no caso de extração daquele de terceiros objetos.

Do ponto de vista do proposto controle epistémico, o a informação preservada em meio digital deverá também preencher os requisitos de sumidade e desconfiança, reforçando a necessidade do tratamento devido.

Considerando a hipótese de que as previsões de cadeia de custódia dispostas em lei se apresentarem incompatíveis com as etapas previstas, o reconhecimento expresso de sua existência e condicionamento da validade da prova ao seu cumprimento implica reconhecer também a necessidade da manutenção da cadeia de custódia do vestígio digital, mesmo que em diferentes termos.

O escopo da Cadeia de Custódia é o de evitar “a manipulação, o erro humano, a fraude, enfim, garantir as condições necessárias para que a evidência possa ser obtida, analisada, auditada e valorada, nas etapas subsequentes do processo penal” (ROSA, 2021, p. 403).

O cumprimento da Cadeia de Custódia depende de soluções adequadas ao meio digital. A preocupação com a segurança e integridade do armazenamento de informações é inerente ao funcionamento meio digital decorrente da natureza volátil, imaterial e frágil dos dados.

São empregadas soluções técnicas para permitir a segurança do armazenamento e transferência de dados informáticos. A quantidade imensurável de interações locais e globais realizada não seria possível sem um padrão seguro que permitisse confiar na integridade dos dados.

A solução adotada quase de maneira universal é a criptografia, que tem como objetivo principal a garantia de confidencialidade, integridade, autenticidade e não repúdio para comunicação segura entre múltiplas partes, considerando a presença de atacantes ou adversários (DONEDA; MACHADO, 2019, p. 8 e ARANHA, 2019, p. 23).

Os objetivos da criptografia se assemelham a da cadeia de custódia. A integralidade e autenticidade são inerentes a confiabilidade da informação e o não repúdio, consistindo na impossibilidade de negar a declaração depois de realizada, implicando enfrentar o problema da fragilidade da informação digital com o instrumento da criptografia.

A cadeia de custódia, no mesmo sentido, enquanto instituição do processo penal, também busca garantir a integralidade e autenticidade da informação que irá integrar o processo.

O progresso das técnicas criptográficas modernas é promovido pela continua procura por vulnerabilidade nas técnicas utilizadas, visando a substituição por práticas mais seguras buscando maior resistência aos adversários mais capazes (ARANHA, 2019, p. 24).

A criptografia em si é bem antiga. Há registro de criptografia simétrica desde época das guerras helênicas, com sua utilização original relacionada a fins militares. Júlio César utilizava o alfabeto cifrado, substituindo cada letra de uma mensagem pela terceira letra subsequente do alfabeto. Era exigido de o destinatário ter a chave para quebrar o código cifrado, no caso seria o prévio conhecimento do número exato de letras que foi avançado (MENKE, 2019, p. 131).

A criptografia assimétrica, consiste num método que utiliza duas chaves, uma aplicada pelo remetente e outra pelo receptor. Há uma chave privada de domínio exclusivo do titular e uma chave pública amplamente divulgada.

Quando o remetente aplica sua chave privada ao assinar uma mensagem, o receptor aplica a chave pública do remetente para verificar a origem. A segurança do método depende da dificuldade de derivar a chave privada da pública (MENKE, 2019, p. 132).

A criptografia assimétrica permite a comunicação confiável entre interlocutores que não se conheçam previamente (MENKE, 2019, p. 133).

O cerne da segurança de um algoritmo criptográfico é um problema computacionalmente difícil, em que um ataque com sucesso à técnica criptográfica implica resolvê-lo a partir do resultado. São empregadas funções fáceis de calcular em uma direção, mas difíceis de inverter, sendo mais eficiente encriptar a chave correta do que encontrá-la por um ataque bruto. A título de exemplo, uma função que multiplica vários números primos grandes é muito mais rápida que encontrar todos os fatores de um número inteiro muito grande (ARANHA, 2019, p. 26).

Os pontos passíveis de intervenção por um atacante são chamados de superfície de ataque de um sistema. Erros de programação e vulnerabilidades do *software* prejudicam a segurança. Defeitos na implementação do algoritmo ou nos processos anteriores ao processamento criptográfico são exemplos de vulnerabilidades que prejudicam a segurança potencial da criptografia, razão pela qual é preferível simplificar os sistemas para diminuir a superfície de ataque e consequentemente elevar a segurança (ARANHA, 2019, p. 27).

A maioria dos protocolos criptográficos modernos é classificada como fim a fim. Calcular e armazenar chaves criptográficas apenas nas pontas da comunicação reduz a ameaça de pontos intermediários ou de ataques por aqueles que operam o serviço e detêm acesso privilegiado, sustentando uma segurança mínima de que os sistemas informáticos necessitam para operar (ARANHA, 2019, p. 28).

A criptografia fim a fim oferece ao usuário um seguro tráfego de informações em rede, porém tão relevante quanto é a criptografia de dados em repouso.

A criptografia em repouso é aquela que cifra informações persistentemente armazenadas em um dispositivo informático, tornando os dados armazenados inteligíveis a terceiros não autorizados (DONEDA e MACHADO, 2019, p. 153).

Os dados podem ser tanto encriptados localmente pelo usuário ou remotamente em servidores diversos. Ressalva-se que a cifragem não decorre somente por parte dos fornecedores de soluções de armazenamento e processamento de informações remotas, serviço também chamado de computação em nuvem, não impede o próprio usuário encriptar os dados antes de carregá-los em servidores (DONEDA e MACHADO, 2019, p. 154).

O principal objetivo é impedir a interferência externa sobre a comunicação, seja a cópia de informações trocadas ou a adulteração de seu conteúdo (ARANHA, 2019, p. 30). Assim, entram em conflito com o interesse investigativo de captura e armazenamento, sendo recorrentemente sugerido forçar a adoção de protocolos menos seguros que possibilitem a interceptação autorizada das comunicações (ARANHA, 2019, p. 31).

Os aplicativos de trocas de mensagens que investem em criptografia fim a fim tornam impossível ao provedor decodificar o conteúdo das mensagens. Tentando circundar as dificuldades técnicas, os investigadores se valem de estratégias para acesso do conteúdo. Ao ignorarem a dicotomia contraditória entre vulnerabilidade e integridade, acabam cometendo erros e prejudicam suas investigações, mesmo atuando de modo legitimo.

A imposição de falhas intencionais para fins de investigação não encontra vantagem real, contraditoriamente só trazendo prejuízos a qualidade da informação eventualmente obtida e a efetividade em coibir crimes que tal medida possa ter.

Desvirtua a razão para a adoção de criptografia, visto que deixa de ser um meio seguro para armazenamento e comunicação de informações e abre flancos de vulnerabilidade a ataques externos. Ao desvirtuar a segurança criptográfica para

acesso à informação, incorre também em retirar a garantia de integridade e confiabilidade conferida pelo seu uso, de modo a tornar imprestável como prova o vestígio obtido.

Também subestima a capacidade dos investigados em procurar meios alternativos para escapar da vigilância investigativa. Um mínimo de informação técnica já permite ao usuário detectar interferências indevidas, sendo bem provável esperar que os investigados tomem cuidados de se afastar de meios que possibilitem a vigilância investigativa, inclusive criando o incentivo para que construam os próprios sistemas.

As técnicas de criptografia são de conhecimento aberto e podem ser facilmente adaptados em infraestruturas particulares, sendo que as falhas introduzidas intencionalmente iriam afetar apenas os usuários legítimos (ARANHA, 2019, p. 33).

Há previsões legislativas no sentido de obrigar os agentes a prestar assistência as autoridades no contexto de investigações criminais. O código penal francês, por exemplo, prevê como crime de obstrução de justiça recusar-se a fornecer a chave criptográfica em sua posse e que possibilite decifrar informação relacionada à preparação, facilitação ou comissão de crime, punido com 5 anos de prisão e multa de até 450 mil euros (LIGURI FILHO, 2019, p. 97).

O Irã de outro modo, criminaliza desde 2009 a criptografia que possa impedir acesso de indivíduos autorizados, salvo autorização expressa do governo (LIGURI FILHO, 2019, p. 99).

Em 2008 o Tribunal Constitucional Federal Alemão (*Bundesverfassungsgericht*) entendeu por reconhecer a confidencialidade e integridade de sistemas de tecnologia da informação como direito fundamental (DONEDA e MACHADO, 2019, p. 9).

Mas isso não impediu a Alemanha de regulamentar a exploração de vulnerabilidades de *software* ou *hardware* por autoridades governamentais para fins de monitoramento e acesso a dados de maneira legitima em investigações (LIGURI FILHO, 2019, p. 102).

Em razão da natureza universal da *internet*, as comunicações entre usuários de diferentes países estarão tão seguras quanto for permitido pelo país menos seguro (LIGURI FILHO, 2019, p. 103). A preocupação quanto ao tratamento externo da criptografia impacta todos os usuários, independente da nacionalidade.

Mas a busca pelo equilíbrio entre acesso legitimo dos dados e a integralidade deles depende de asseveração de riscos dentro de uma sociedade. A tipificação penal é resultado da busca em diminuir os riscos potenciais de indivíduos, criminalizando determinadas condutas para resguardar objetos jurídicos que se elenca como relevantes. O processo penal, integrando assim as práticas investigativas e constituição de elementos probatórios, concretiza a expectativa depositada na tipificação penal (SALVADOR NETTO, 2006, p. 89, 94 e 97).

Se foram elencadas garantias constitucionais protegendo a privacidade e a presunção de inocência, de igual grandeza se reveste o juízo de legitimidade para eventual mitigação destas proteções.

Os limites na investigação devem levar em conta os contornos sociais da tipificação penal. Se há justificativa indiscriminada para devassa na vida privada de todos os indivíduos ante a potencial ilicitude de suas condutas, significa que as normas penais perderam sentido, visto que a regra da sociedade é a potencialidade de condutas tidas como delinquentes, mas factualmente aceitas e habituais.

Ainda que haja um reflexo universal nas decisões tomadas frente a problemática segurança e privacidade na investigação, prevalece o respeito ao arcabouço interno de garantias e risco plural dos Estados. Posto isto, consenso no internacional quanto a parâmetros mínimos de segurança digital foge a razão lógica técnica, atingindo a alçada da autodeterminação de Nações Soberanas.

Porém, a paridade universal de acesso a soluções criptográficas vem a tornar obsoleta decisões legislativas que ignoram suas particularidades. O arbítrio do Poder Estatal, por mais déspota que seja sua forma de governo, encontra limites na realidade. A legislação pode prever o impossível, mas sua positivação não pressupõe efetividade.

Se o avanço tecnológico é inevitável, cabe ao legislador acompanhar as mudanças. A resistência à adaptação leva ao obsoletismo, a ingerência na capacidade em encontrar soluções adequadas à realidade.

Levanta-se a possibilidade de trazer as informações digitais como documento ao processo. O Código de Processo Penal (BRASIL, 1941) define que poderão ser apresentados documentos em qualquer fase do processo, definindo-os no *caput* do artigo 231 como “quaisquer escritos, instrumentos ou papéis, públicos ou particulares”.

Antonio Magalhães Gomes Filho (2019, p. 474-475) defende que diante de uma nova realidade tecnológica, deve ser expandido o conceito restritivo de

documento adotado pelo Código de Processo Penal para abranger como documento “qualquer objeto material que contenha símbolos capazes de comunicar algo em relação a um determinado fato, permitindo chegar ao conhecimento desse mesmo fato” e que só será realizada perícia quanto houver dúvidas quanto a veracidade do documento, nos termos do artigo 235 (BRASIL, 1941).

Nesse sentido, Guilherme Madeira Dezem (2019, p. 705) aponta que a partir da alteração promovida no Código de Processo Penal em 2008, deve ser entendido o documento nesse conceito amplo de prova documental.

Foi incluindo no artigo 479, atinente aos debates dentro do procedimento de júri, a restrição da leitura de documento ou exibição de objetos não juntados tempestivamente aos autos no julgamento, ressalvada no parágrafo único que a proibição aplica-se “a leitura de jornais ou qualquer outro escrito, bem como a exibição de vídeos, gravações, fotografias, laudos, quadros, croqui ou qualquer outro meio assemelhado, cujo conteúdo versar sobre a matéria de fato submetida à apreciação e julgamento dos jurados” (BRASIL, 1941).

Como apresentado, a garantia de integridade e confiabilidade de informações armazenadas em meio digital depende de procedimentos técnicos. A apresentação sob a égide da classificação como documento se manifesta um potencial artifício para circundar a exigência de Sumidade e Desconfiança para admissibilidade de prova, fugindo a lógica de uma Cadeia de Custódia.

Alexandre Morais da Rosa (2021, p. 437-439) também defende a amplitude da prova documental, porém ressalva a necessidade de se ater as características de vulnerabilidade e fragilidade da prova digital, devendo ser obedecida as normas técnicas para sua extração e tratamento para sua admissibilidade probatória.

Diferentemente do processo civil, a demonstração de validade e eficácia no processo penal é atribuída à acusação, não produzindo qualquer efeito probatório se a prova não demonstrar regularidade, não havendo consolidação da verdade pela não impugnação.

Assim, não haveria inadmissibilidade da prova digital enquanto documento desde que respeitado os quesitos técnicos atinentes à sua orientação e tratamento (ROSA, 2021, p. 437).

A prova digital documental deve ser orientada enquanto meio adequado para provar o que se é alegado, demonstrar equivalência entre o que representa e o conteúdo verificável e expor elementos suficientes para superar testes de verificação.

Deve ser adquirido através da cópia integral, capacitando as partes auferir condições de audibilidade da metodologia e procedimentos adotados, a repetibilidade dos resultados obtidos, a equivalência dos resultados por meio de instrumentos diversos e a justificação dos métodos utilizados para extração, obtenção e processamento dos dados (ROSA, 2021, p. 437, 438).

Deste modo, o procedimento de documentação digital deve também respeitar a Cadeia de Custódia para admissibilidade enquanto prova, é dever de todos os agentes que participam na obtenção ou tratamento de informações armazenadas em meio digital. Deve haver o “controle de obtenção, movimento e acesso aos dados, com a identificação, histórico de acesso, por tempo, local e motivação, além de eventuais alterações” (ROSA, 2021, p. 438).

3.1 Acessibilidade de dados

É invocada a presunção de inocência como um princípio contrário a vigilância pois, além da violação de privacidade, implicaria em uma criminalidade implícita dos indivíduos (HADJIMATHEOU, 2020, 24). Uma desconfiança geral na autodeterminação individual em cumprir a lei, racionalizando ao Estado, em prol da segurança pública, obter acesso a vida privada das pessoas para protegê-las de infratores, tratando todos igualmente como inimigos em potencial.

Cautela não implica na desconfiança generalizada ou violação de privacidade. O mero monitoramento ou restrição de acesso mediante a apresentação de determinados documentos ou registro não são discriminações pessoais, mas sim medidas cautelares de segurança, preventivamente reduzindo o risco de incidentes.

É possível até entender que a coleta rotineira de informações poderia dar acesso à defesa dos acusados de provas que não teria de outro modo, possibilitando melhor exercício do ofício e diminuindo os erros judiciais (HADJIMATHEOU, 2020, p. 36-40).

Não se nega o potencial da vigilância em diminuir o escopo de risco dentro do processo penal, observando o interesse da defesa na atividade probatória. Mas voltando a questão da asserção de risco na sociedade, se há opção pelo resguardo da privacidade, não parece lógico suprimi-la como regra. Não há crime inerente ao agir às escuras.

A ilicitude do anonimato só se caracteriza quando utilizado para abuso do livre exercício da manifestação de pensamento. O estado não identificável nem localizável é protegido pela privacidade, enquanto direito de defesa da individualidade e da personalidade humana frente a intromissões indevidas ou determinações sobre vidas alheias, sendo completamente lícito navegar anônimo na *internet* (TENORIO, 2020, p.150-153).

Assim, a hipótese de uma vigilância contínua do conteúdo acessado através da *internet* ou de dispositivos informáticos alheios como regra, em razão de prevenir delitos, sem qualquer autorização ou motivação prévia, não parece razoável intromissão estatal em um Estado de Direito.

Especificamente quanto as comunicações, a Constituição Federal (BRASIL, 1988) impõem em seu artigo 5º, inciso XII, a inviolabilidade do sigilo das comunicações telegráficas, de dados e telefônicas, com a ressalva quanto a

possibilidade de quebra do sigilo das comunicações telefônicas para investigação e instrução criminal.

Entende-se que o que é inviolável é fluxo das comunicações enquanto ela ocorre, não atingindo a mesma proteção ao conteúdo armazenado das comunicações nem os metadados gerados por elas (ABREU e ANTONIALLI, 2019, p. 59).

O acesso a dados de comunicações privadas armazenados por intermediários, como no caso de provedores de aplicações de *internet*, é condicionado a ordens judiciais, no termo do artigo 7º, inciso III, do Marco Civil da *Internet* (BRASIL, 2014).

A referida lei dispõe obrigação de armazenamento de metadados pelos provedores de conexão e aplicações de *internet*. O artigo 5º define que registro de conexão é o conjunto de informações referentes à data e hora de início e término de uma conexão à *internet*, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" e o registro de acesso a aplicações de *internet* é o "conjunto de informações referentes à data e hora de uso de uma determinada aplicação de *internet* a partir de um determinado endereço IP" (BRASIL, 2014).

O provedor de conexão deve guardar os dados pelo prazo de 1 ano e o de aplicações por 6 meses, sendo que, em caso de pedido cautelar do Ministério Público ou de autoridade policial, esse período pode ser estendido até que eles obtenham a autorização judicial para acesso aos registros. (BRASIL, 2014)

De outro modo, nada impede o acesso a dados cadastrais, de maneira administrativa, pelas autoridades que detenham competência legal para sua requisição (QUITO, 2020, p. 175).

A coleta e tratamento de dados é limitada pelo Marco Civil da *Internet* e a Lei Geral de Proteção de Dados (LGPD), exigindo consentimento expresso do usuário e incentivando a exclusão dos dados. Assim, há uma impossibilidade de se fornecer os dados não coletados e os excluídos. Porém, em contrário senso, quaisquer dados coletados e atualmente armazenados pelo provedor de serviços podem ser entregues mediante autorização judicial (BARBOSA e MOURA, 2020, p. 496).

A LGPD (BRASIL, 2018) em seu artigo 3º expressamente excluiu a sua aplicação para atividades de investigação e repressão de infrações penais, devendo ser regida por legislação específica e respeitando os princípios gerais elencado na lei.

Assim, cabe observá-la quanto as possibilidades e exigências aos tratamentos de dados para nortear o que é possível.

O registro do tráfego das mensagens se limita a metadados, como data, duração e quantidade de dados trafegados, sendo impossível o atendimento por parte do provedor de serviço a interceptação ou a entrega do conteúdo da mensagem (QUEIROZ, 2019, p. 36).

Aplicativos de mensagens instantâneas excluem os metadados de imagens compartilhadas dentro de seus sistema e plataformas de serviços podem apagar conteúdos que vão contra suas diretrizes, ficando a prova sujeita a se perder (NASCIMENTO, 2020, p.123).

O artigo 22 do Marco Civil da *Internet* (BRASIL, 2016) condiciona a viabilização do fornecimento de dados capaz de identificar um usuário à delimitação na requisição de fundados indícios de ocorrência do ilícito, motivação da utilidade dos registros solicitados para investigação/instrução e o período ao qual se referem os registros necessários. A requisição, seja para instrução probatória criminal ou cível, será submetida pelo interessado à reserva de jurisdição.

Devido ao alto valor comercial do tratamento de dados, as empresas têm o costume de armazenar e trabalhar dados, seja para melhoramento de seus serviços ou oferecê-los a outros interessados, podendo fazer recortes diversos dos dados pessoais processados para atender interesses diversos. Entre eles, atribui-se maior relevância aos dados de localização para fins investigativos.

Problemática se reveste quanto a requisitar dados de localização em massa para investigação reversa, de todos os usuários registrados em determinado local e data para extrapolar por eliminação o suspeito de crime determinado.

Justificam ser somente modesto o prejuízo a intimidade individual das pessoas afetadas pois somente atinge a localização momentânea do aparelho (BARBOSA e MOURA, 2020, p. 497), porém, a título de exemplo do mencionado na introdução do caso Dinamarquês, a baixa acurácia das informações coletadas pode levar a erros judiciais severos se não houver a devida diligência dos investigadores quanto aos dados recebidos.

Pela natureza descentralizada do armazenamento digital de informações, os dados se espalham por diversos servidores sujeitos a diversas legislações locais. Com certa regularidade, o provedor de serviços responsável pelos dados mantém sua sede no exterior e a filial no Brasil. A filial afirma não ter posse dos dados e a matriz que

está impedida de fornecê-los somente por ordem judicial no país de origem, levando às autoridades brasileiras ter de recorrer à assistência judiciária internacional.

A convenção de Budapeste, cujo Brasil foi convidado a aderir em 2019 e atualmente está em tramitação no Senado Federal sob a alcunha de Projeto de Decreto Legislativo nº 255/21, prevê a possibilidade de exigir diretamente às filiais nacionais de provedores de serviços estrangeiros dados cadastrais em seu controle relativos aos serviços, facultando ao direito interno a ordem para que comunique os dados na sua posse ou controle (BARBOSA e MOURA, 2020, p. 500).

Os dados podem ser protegidos por credenciamento para acesso ou negados acesso pelo possuidor, exigindo operações de busca e apreensão para obtê-los. Existe, de outro modo, uma ampla gama de informações e fontes disponíveis ao público em fontes abertas, disseminadas sem obstaculizar seu acesso (NASCIMENTO, 2020, p. 114-115).

As informações coletadas em fontes abertas também têm um amplo espectro de qualidade e veracidade, não havendo necessariamente um critério para sua disponibilização além de consentimento provedor e do usuário que as disponibilizam.

É possível considerar que informações disponibilizadas em fontes oficiais de instituições públicas, como o portal de transparência, teriam uma presunção de veracidade.

Porém, mesmo apresentando elas como fonte, necessitam devida atenção ao serem reproduzidas no processo. Não há como atestar sua integridade e origem sem a devida diligência por parte do responsável pela investigação, seja o órgão acusador ou a defesa.

A informação disponibilizada na *internet* pode estar alocada em servidores a cargo de terceiros, indiferente a relevância dela ou apagá-la intencionalmente. Há alguns serviços como o *Save Page Now* do *Internet Archive* (2021) que geram links permanentes, registrando o estado de uma página da *internet* em determinado momento (NASCIMENTO, 2020, p.122).

Esses *links* permanentes atribuem um *timestamp*, uma marca de tempo, à informação e preservam do modo que se apresenta naquele recorte temporal, evitando a perda dela com o decurso do tempo.

São ferramentas importantes para constatação da existência em determinado momento de um fato jurídico relevante. Mas tais soluções se limitam a certificar uma

declaração de estado daquele conteúdo em determinado tempo, não havendo concreta extração dos dados lá alocados.

Quanto a operação de dados em nuvem, outros problemas de origem técnica surgem para a extração forense dados. Os serviços em nuvem dependem do acesso a servidores externos para operar os aplicativos de *internet*, muitas vezes operando com a simulação de múltiplos ambientes virtuais particionados de um único dispositivo físico.

Usuários de serviços de *software* tem pouco ou nenhum controle sobre a localização física de seus dados. Os dados são catalogados em grande volume e em formatos proprietários da plataforma. A diversidade e número de máquinas virtuais em uma única máquina física faz com que seja difícil separar recursos sem quebrar confidencialidade dos usuários, fazendo com o que os registros vulneráveis facilitem atacantes esconderem seus traços. Instancias de servidores rodando em máquinas virtuais na nuvem são monitoradas por hipervisores, programas de gerenciamento de múltiplas máquinas virtuais.

O descuido com procedimentos e ferramentas para investigação forense, mesmo com muito progresso da pesquisa na área, revela que os métodos tradicionais são inadequados para a nuvem. A investigação digital tradicional não tem muito apreço para a questão de retenção e integridade da extração dos dados. Há proposições no sentido da necessidade de coletar dados do sistema operacional na camada inferior das máquinas virtuais, coletando relatórios completos, confiáveis e capazes de operar na arquitetura da nuvem, possibilitando a análise forense (LIU; SINGHAL; WJESEKERA, 2017).

É tecnicamente viável o uso de *softwares* espiões instalados de forma oculta nos dispositivos dos investigados (BARBOSA e MOURA, 2020, p. 484), porém também incorre no problema dicotômico previamente apontado: a vulnerabilidade explorada retira a segurança de integridade dos dados acessados. O *software* utilizado dependeria de controle delimitado o seu método de acesso e como ele extrairia os dados, de modo a possibilitar a auditabilidade do procedimento, preferencialmente com o mínimo de intervenção humana possível.

O Código Penal (BRASIL, 1940), no artigo 154-A, tipifica a invasão de dispositivo informático mediante violação de mecanismos de segurança para acesso e manipulação de dados indevidamente ou instalar vulnerabilidade para obter

vantagem ilícita, bem como o desenvolvimento e distribuição de aplicativos capazes de possibilitar tal prática.

Observa-se que o delito descrito condiciona a ilicitude à falta de justificativa idônea, o que não impediria o desenvolvimento de aplicativo para invasões idôneas para quebra dos mecanismos de segurança devidamente fundamentados e condicionadas à reserva legal.

Também é totalmente possível obter o conteúdo em questão mediante busca e apreensão de qualquer dos aparelhos envolvidos sem que tenha que se comprometer a integridade e confiabilidade das informações extraídas (ALIMONTI, 2019, p. 64).

O artigo 240, §1º, do Código de Processo Penal (BRASIL, 1941) prevê a busca e apreensão, devidamente fundamentada, para descobrir objetos necessários à prova e colher elementos de convicção.

O mandado de busca não autoriza a devassa nas informações pelo investigador, porém possibilita a sujeição do dispositivo informático à perícia técnica. Ante as recorrentemente referidas particularidades do armazenamento informacional em meio eletrônico, o acesso pelo agente policial ao dispositivo informático causa indevido comprometimento a integralidade dos dados lá alocados, abrindo margem para dúvida na medida que o último acesso registrado ao dispositivo é do agente policial e este teve a possibilidade de manipular os dados.

A diligência, como a regra das medidas cautelares penais, pressupõe a existência *periculum in mora* e *fumus delicti commissi*. O perigo na mora, o risco de desaparecimento ou ocultação do vestígio digital é inerente as suas características, principalmente quando a volatilidade e fragilidade. A probabilidade do cometimento do delito e de que a diligência encontrará elementos de prova pode ser adequadamente fundamentada.

Para validade da busca, o mandado deve ser específico quanto ao objeto a ser apreendido, vinculada à fundamentação da autorização judicial (ROSA, 2021, p. 396-397). Mesmo que legitima e objetiva a apreensão, resta dúvida quanto ao escopo admitido para diligência sobre os dados.

O dispositivo é apreendido para acesso a dados relacionados determinado crime, mas, pela própria versatilidade inerente aos dispositivos informáticos, não é instrumentalizado especificamente à determinada tarefa ilícita, de modo a armazenar dados diversos.

Em razão de diminuir o viés cognitivo, a integralidade dos dados disponíveis deveria ser objeto de extração de dados. De outro modo, não se justifica a devassa expansiva e desnecessária sobre a privacidade individual.

O procedimento operacional padrão (SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA, 2013, p. 88-89) prevê que depois da duplicação da mídia original do dispositivo, é realizado o processamento e análise de dados, seguindo a extração direta dos arquivos relacionados ao escopo pericial.

Fica sob responsabilidade do perito a escolha do que é potencialmente interessante à investigação e consequente interesse probatório. Há, portanto, margem para arbitrariedade nas informações apresentadas no laudo.

Contrário à disposição técnica procedimental, se mostra necessário submeter ao contraditório quais arquivos deverão ser selecionados como relevantes, não ao crivo do perito.

Se a prova é de propriedade neutra das partes, cabe a elas defenderem a delimitação da relevância. A disposição integral dos dados permite exercer a paridade de armas entre defesa e acusação, diminuindo a assimetria informacional.

De outro modo, a disposição integral dos dados irrelevantes pode trazer constrangimentos desnecessários à esfera pessoal do investigado ou até mesmo a descoberta de elementos de crime não necessariamente relacionados à conduta que autorizou a apreensão do dispositivo diligenciado.

Quanto a serendipidade, o encontro fortuito de vestígios relacionados a crimes diversos, prevalece a necessidade da acusação de comprovar vinculação dos elementos colhidos com o delito que fomentou a diligência (ROSA, 2021, p. 398).

Ainda que se defenda o exercício do contraditório diferido, exercido já na fase judicial, para a delimitação da seleção de relevância dos vestígios digitais colhidos, é possível particionar a mídia de modo a resguardar a privacidade e garantir a integridade dos elementos.

Na diligência, após o espelhamento da mídia original, poderia ser realizada cópias particionadas subsequentes, separando os elementos tidos pelo perito inicialmente como relevantes e os irrelevantes.

A cópia integral e fiel ao conteúdo original seria guardada para eventual confronto posterior, a mídia com os arquivos selecionados como relevantes seria juntada aos autos e a mídia com o conteúdo considerado como irrelevante restituído ao investigado.

A hipótese apresentada equilibraria o acesso legítimo a informações armazenadas em meio digital aptas a serem admitidas como provas, ao mesmo tempo que resguarda maiores devassas na vida pessoal do investigado, inclusive possibilitando o acesso a arquivos não relacionados a investigação, podendo inclusive selecionar conteúdo que ele entenda relevante para sua defesa não selecionado pelo perito.

Os artigos 10-A a 10-D da Lei 12.850/13 (BRASIL, 2013), bem como os artigos 190-A a 190-E do Estatuto da Criança e do Adolescente (BRASIL, 1990), preveem a infiltração de agentes policiais para investigação de delitos relacionados a organização criminosa e contra a dignidade sexual de crianças e adolescentes, condicionada a autorização judicial e na falta de possibilidade de produção de provas por outros meios.

A infiltração possibilita ao agente policial colher informações através de identidade fictícia. A prática cria oportunidades conquistando a confiança dos criminosos, seja pela obtenção de informações sigilosas espontaneamente compartilhadas com o agente ou pela exploração de vulnerabilidades decorrentes da confiança, facilitando o acesso a dispositivos informáticos para extração de dados.

Tratando-se da paridade de armas informacional, ao mesmo tempo que os agentes públicos têm à sua disposição a possibilidade de requisição direta de informações, é possível a defesa se valer da Lei de Acesso à Informação (BRASIL, 2011) para acesso a informações coletadas pelo poder público.

Não é possível se utilizar do recurso para obter informações privilegiadas sobre diligências em andamento que demandem sigilo, porém é plenamente efetiva para garantir ao requerente acesso a informações relativas a investigações que o vinculem a atos ilícitos (ROSA, p. 442).

A referida legislação permite ao requerente acesso a informações sob o domínio de agentes e instituições estatais, potencialmente relevantes à sua defesa. Através de sua invocação é possível expandir as arestas relativas a própria investigação, exigindo a apresentação registros e justificativas dos atos investigatórios que de outro modo não se revelariam no processo.

A atuação dos investigadores é orientada a coleta de elementos probatórios para fundamentar uma justa causa e consequentemente possibilitar a condenação do investigado. Saltos lógicos no procedimento podem indicar fontes ocultas de prova não trazidas aos autos, seja pela sua ilicitude ou inconsistência com a narrativa

convencionada, de modo que acesso a dados periféricos sobre a investigação são um meio de revelar tais ingerências à defesa.

3.2 Qualidade dos dados extraídos

O mero acesso aos dados é insignificante se a precisão e confiabilidade das informações ofertadas não atingirem um patamar mínimo para seu uso. Se o meio de extração dos dados pode vir a interferir em sua qualidade, a origem tem ampla influência na capacidade informativa que eles podem oferecer.

Os dados podem ser espoliados, sujeitos a degradação por incidência de elementos externos, como calor, umidade e campos eletromagnéticos, ou adulterados pela violação da integridade e auditabilidade (ROSA, 2021, p. 438).

A possibilidade de acessar e trabalhar dados de maneira legitima não impede a distorção ocasionada pela ignorância do escopo da informação apresentada. A título de exemplo, dados de localização tem abissal diferença em precisão se obtidos via registro das antenas telefônicas ou pelo sistema de GPS (*Global Positioning System)* incorporado ao aparelho.

As antenas chamadas de Estações Rádio Base (ERB) são responsáveis pela comunicação móvel, integrando a infraestrutura de rede móvel, recebendo e enviando informações aos dispositivos móveis e conectando-os a outras redes através do serviço da empresa prestadora de serviços (SANTOS e VALE, 2020, p. 80-86).

Os dados de localização que podem ser fornecidos pela empresa de telecomunicações compreendem apenas a aproximação da localização do dispositivo móvel baseada na triangulação e trilateração da comunicação do sinal entre torre e dispositivo móvel.

A aproximação é calculada levando em conta a intersecção do sinal por três torres adjacentes e a análise da força do sinal recebido pelo dispositivo, o que leva a margens de erro de centenas de metros ante o amplo espectro de variantes e interferências causadas em cada área de cobertura das ERBs.

O sistema de localização por GPS chega a ter a margem de erro de míseros centímetros. A localização é auferida através da triangulação com satélites em conexão contínua, informando localização em deslocamentos em tempo real. Porém, o acesso a esse tipo de dado depende da disponibilidade ao dispositivo de um serviço de conexão de dados móveis e o sinal do GPS estar ativado pelo usuário.

O acesso e monitoramento desses dados exige a intervenção remota ou física no dispositivo em questão. Eventual armazenamento destes registros em plataformas online obtidos pela quebra de sigilo pode sofrer inconsistências determinadas pelo

interesse e natureza da exploração comercial do serviço, inclusive a possibilidade de o próprio usuário manipular os registros a seu próprio interesse.

Coloca-se ainda que não há garantia da identidade física do portador do dispositivo informático. A contratação de serviços pode ser realizada através de cadastros de terceiros e não necessariamente existe um usuário exclusivo do dispositivo, podendo gerar distorções na interpretação dos dados auferidos.

Não há, ainda, necessária conferência das informações cadastrais fornecidas pelos usuários por parte dos provedores de aplicação, de modo que a própria utilização de dados por eles providos se faz temerária se não acompanhada dos metadados relativos à conexão e uso dos serviços (BLUM e TAMER, 2020, p. 583).

Sistemas de vigilância audiovisual também se mostram muitas vezes vulneráveis a racionalidade falaciosa. As câmeras de segurança têm três objetivos principais: preventivo relativo à capacidade de evitar crimes futuros, reativo quanto a capacidade de permitir a efetiva atuação policial repressiva, e probatório, relacionado a capacidade de juntar elementos que fundamentaram a investigação e consequente condenação do delinquente (OLIVA, 2020, p. 140-145).

A função preventiva se esgota com a adaptação e desenvolvimento de novas práticas criminosas após identificada a presença da vigilância eletrônica.

Os operadores não têm capacidade de dar atenção a todas as câmeras ao mesmo tempo e há um limite a disponibilidade de agentes para responderem imediatamente os alertas de monitoramento, sendo raro os casos de prisão em flagrante em razão do monitoramento e consequentemente não se justificando na função repressiva.

Resta efetiva a função probatória em relação a crimes cometidos sob e registrados pelas câmeras. Porém, as câmeras são operadas por pessoas, podendo influenciar o monitoramento em razão de suas irracionalidades, disfuncionalidades e preconceitos (OLIVA, 2020, p. 147).

Se faz necessário a apreciação integral dos registros de imagens realizados pelo sistema de vigilância inteiro, não somente às câmeras apontadas como relevantes à investigação, extraídas também diretamente sobre o aparato de armazenamento das imagens para evitar vulnerabilidades no procedimento de acesso aos dados.

Os dados armazenados em um sistema de vigilância digital alcançam volumes astronômicos de dados dependendo da quantidade de câmeras acopladas. Se por um

lado nem todos os registros são relevantes à investigação penal, não é possível excluí-las sem submetê-las ao contraditório.

O recorte acusatório pode esconder elementos relevantes do fato, intencionalmente ou não, ao se limitar a utilizar os registros restritos ao tempo e local do fato denunciado, ignorando eventual registro de aspectos relevantes no mesmo sistema nas imediações ou locais distintos, como uma causa de exclusão de ilicitude, por exemplo.

Os sistemas de vigilância operam e registram as imagens em formatos próprios de armazenamento, para garantir integridade e eficiência da catalogação e disposição dos registros, mantendo informações relevantes ao monitoramento, como de qual câmera se origina e a possibilidade de sincronizar a visualização concomitante de registros de outras câmeras.

No processo de exportação das imagens para fora do sistema de vigilância, momento que se atribuí um formato armazenamento de ampla acessibilidade, essas informações periféricas são perdidas se não corretamente extraídas. Assim, sem a extração direta do sistema de vigilância por profissional técnico ou mesmo o espelhamento integral da operação para análise, esvazia-se a integridade do vestígio.

Como se observa no precedente do Recurso em Habeas Corpus nº 99.735-SC (BRASIL, 2018), a prova se torna ilícita se não é possível assegurar sua integridade.

No caso, os policiais, com autorização judicial, apreenderam o aparelho celular do réu e habilitaram o recurso *Whatsapp web*, permitindo o acesso remoto das mensagens trocadas no aplicativo *Whatsapp,* restituindo em seguida o aparelho ao investigado.

Ocorre que o recurso habilitado também permitia enviar e excluir as mensagens por parte dos investigadores, sem qualquer registro das alterações, razão pela qual foi concedida a ordem por unanimidade.

Alexandre Morais da Rosa (2021, p. 395) inclusive aponta a ilegalidade da própria prática de espelhamento remoto de aplicativos de troca de mensagens, visto que seria uma modalidade de *fishing expedition,* o encontro fortuito dissimulado e indiscriminado por parte da investigação para subsidiar futuras acusações de crimes ainda desconhecidos. .

Volta-se ao problema da exploração de vulnerabilidades para acesso a dados: o rompimento do sistema de segurança permeia a integridade dos dados obtidos. A

mera possibilidade legitima de obter os dados com o uso de métodos ocultos não legitima a prova colhida.

Se não for possível limitar a manipulação dos dados pelo agente responsável pela invasão, a prova se torna ilícita. Para auferir capacidade de *onus probandi* da prova colhida por tais meios seria necessária a delimitação do procedimento da ferramenta de modo claro e utilizando recursos que evitem maiores ingerências humanas, como a automatização da extração após determinado o dispositivo alvo.

O esclarecimento dos modos utilizados incorre em uma contradição técnica: se expostos os métodos ocultos, menos efetividade terão nas incursões futuras, justamente pelo desenvolvimento de estratégias diversas pelos infratores para escapar de seu escopo.

Observa-se que se de um lado a utilização dos métodos acima como prova sofrem limitações da parte técnica para auferir integridade e legitimidade aos dados obtidos, não se impede que sejam utilizados para inteligência investigativa.

Havendo legitimidade nos métodos adotados, seja pela quebra de sigilo de dados autorizada judicialmente ou a intervenção oculta em dispositivos informáticos, mesmo que resultem em dados sem utilidade probatória, a possibilidade de serem utilizadas como meio de investigação se mostram suficientes.

A título de exemplo, na hipótese de uma ameaça realizada por um aplicativo de troca de mensagens, o *printscreen* apresentado pela vítima à autoridade policial poderia justificar a abertura de inquérito e fundamentar a requisição de dados relacionados à mensagem perante provedores de serviços de *internet* e até mesmo o deferimento de medidas cautelares urgentes, possibilitando a correta coleta de elementos capazes de fundar a justa causa para viabilizar eventual denúncia.

Porém, no âmbito probatório, aquele *printscreen* não é apto a provar a materialidade e autoria delitiva. Seria necessário a extração dos dados da mensagem diretamente do aparelho da vítima e o confronto dos metadados obtidos pelos provedores de serviços para concreta conclusão da integridade daquele conteúdo bem como de onde se originou, indicando, inclusive, elementos que possam conferir pessoalidade ao usuário daquele dispositivo de onde se originou a mensagem recebida pela vítima.

Pela própria descentralização inerente ao armazenamento digital de informações, não há garantia de uma diligência em um dispositivo seja suficiente para coletar e extrair todos os dados necessários a confirmar o conteúdo e origem de

determinada prova digital. Mas a devida diligência nas frações de cada elemento vestigial obtido pode vir a compor prova adequada ao processo penal.

Precariedade do elemento digital apresentado inicialmente, seja como notícia crime ou no proceder da investigação, não impede a confirmação dele por outros meios. É inadmissível sua qualidade como prova sem a devida cautela procedimental, porém é pleno seu uso como evidência investigativa se legítima sua apresentação/obtenção.

3.3 Sistemas de autenticação digital

A prova penal tem por escopo a prova de um ato ilícito, podendo ser demonstrada por todos os meios de prova admitidos e lícitos (BADARÓ, 2019, p. 27). Ao mesmo tempo que não se vale da formalidade de prova cível de um negócio jurídico, relacionada muitas vezes a autoridade investida de quem declara sua veracidade, também não exclui a possibilidade de sua utilização como prova penal.

Por aplicação analógica do artigo 411 II, do Código de Processo Civil (BRASIL, 2015), o documento pode ser considerado autêntico quando “a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei”. Deste modo, é possível invocar regras técnicas como argumento de verificação da idoneidade (ROSA, 2021, p. 438), bem como a utilização de sistemas de autenticação previstos no ordenamento jurídico.

Há previsão legal de um sistema de autenticação de documentos eletrônicos. A medida provisória 2.200-2/01 institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), com a finalidade de “garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras” (BRASIL, 2001).

O titular gera um par de chaves criptográficas, vinculadas ao respectivo titular através da emissão de um certificado digital por uma Autoridade Certificadora. Uma chave fica listada sob a gerência da Autoridade Certificadora Raiz (atualmente o Instituto Nacional de Tecnologia da Informação), e a chave privada de assinatura fica sob exclusivo controle, uso e conhecimento do titular.

A referida medida provisória equipara documentos eletrônicos submetidos a infraestrutura posta como documentos públicos ou particulares para todos os fins legais, inclusive presumindo verdadeiras as declarações dos documentos em forma eletrônica subscritos com certificado digital em processo de certificação disponibilizado pela ICP-Brasil. Porém, ressalva que a previsão legal da infraestrutura de certificação não impede a “utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento” (BRASIL, 2001).

Infraestrutura existe para uniformizar o tratamento dos usuários, possibilitando acessá-la e fazer uso dela quando for necessário. Quem adquire um certificado digital

procura identificar a origem ou assinar documentos em meio eletrônico de modo seguro (MENKE, 2019, p. 125-127).

Assim, o referido sistema de autenticidade se volta a registrar a autoria ou convalidação das informações contidas no documento pelo titular ou titulares signatários, garantindo a integridade da declaração da informação alocada no processo de certificação da assinatura digital.

O conteúdo de um documento assinado eletronicamente não é criptografado. O que é efetivamente assinado é a função *hash* (MENKE, 2019, p. 134). O conteúdo continua acessível a todos, sendo cifrado o resumo da mensagem. A autenticidade da certificada resta na declaração, não no conteúdo.

A ressalva quanto a não exclusividade do sistema para comprovação de autoria e integridade de documentos condiciona a validade do documento à aceitação. Deste modo, a lei implica que a garantia de validade dos procedimentos dentro da Infraestrutura de Chaves Públicas Brasileira acaba sendo a autoridade burocrática.

Os procedimentos de certificação e registro das chaves criptográficas ficam submetidas a cadeia hierárquica das Autoridades Certificadoras e seus procedimentos internos. O uso delas também são submetidos a plataformas de certificação disponibilizadas por eles.

A submissão a tais procedimentos, portanto, é a garantia de que o documento em formato digital tem presunção de veracidade de que as informações nele contidas foram declaradas ou convalidadas pelo titular da chave de assinatura utilizada.

Logo, pela lei, qualquer outro procedimento que vise garantir autenticidade do documento em formato eletrônico, mesmo que seu registro de metadados seja robusto o suficiente para permitir auferir e auditar sua integridade e confiabilidade, é condicionado a aceitação de terceiros. Ou seja, sob o escopo legal da referida lei da ICP-Brasil, outros sistemas de autenticação, burocráticos ou não, têm sua validade jurídica vinculada à adesão e não a sua confiabilidade.

Observa-se que o sistema de autenticação é relacionado a declaração do conteúdo, não ao conteúdo em si. Sem elementos das condições originais do conteúdo quanto ao procedimento de aquisição e conservação das informações acostadas, não há elementos para preencher os requisitos de Sumidade e Desconfiança da prova.

Outro instrumento no direito brasileiro tem a mesma função: a ata notarial. A autoridade burocrática confere ao documento valor, não sua integridade.

No âmbito do direito processual civil, houve previsão expressa da figura da ata notarial (art. 384), onde tudo aquilo que pode ser percebido pelo tabelião é passível de ser retratado na ata notarial, registrando o STJ decisões monocráticas no sentido de confirmar sua aptidão para documentar atividade da *internet* (CARACIOLA; ASSIS; DELLORE, 2019, p. 61).

O item 138 das Normas de Serviço da Corregedoria-Geral da Justiça do Estado de São Paulo dispõem que “Ata notarial é narração objetiva, fiel e detalhada de fatos jurídicos presenciados ou verificados pessoalmente pelo Tabelião de Notas”.

O documento público atesta por pessoa de fé pública a origem, os participantes e a veracidade de seu conteúdo, porém a eficiência probatória da Ata Notarial é limitada aquilo que o Tabelião de Notas tiver presenciado e tiver capacidade de compreender (CARACIOLA; ASSIS; DELLORE, 2019, p. 64-65).

O objetivo da ata notarial é a verificação e constatação de existência ou estado de determinado momento de um fato de relevância jurídica por terceiro garantidor de confiança.

Registros públicos servem para estruturar dados de maneira a atribuir publicidade, transparência e autenticidade a certos tipos de transações juridicamente relevantes (CABRAL, 2020, p. 95).

Ocorre que o fato jurídico presenciado pelo Tabelião de Notas é limitado ao que lhe é apresentado. A constatação, por exemplo, da existência de uma mensagem em um determinado aparelho eletrônico ou uma publicação em rede social é relativa e passível de fraudes.

Ao Tabelião é conferida autoridade pública para verificação de fatos jurídicos, mas não capacidade técnica absoluta de constatação de verdade. Se a constatação não incluir os elementos necessários a garantir a integridade e confiabilidade da prova produzida, obedecendo quesitos de Desconfiança e Sumidade em submissão à Cadeia de Custódia, é prejudicada sua admissibilidade.

Se é realizado somente o acesso a determinado conteúdo e declarado sua existência em determinado período, a prova produzida não se demonstra muito diferente da certificação digital.

De outro modo, se realizada com adequada extração dos dados, não mero acesso e confirmação de existência deles, se apresenta como prova capaz no processo penal.

Mais recentemente, com o avanço das tecnologias criptográficas, foi apresentado o *blockchain* como suposta solução de segurança da integridade e confiabilidade do armazenamento digital de informações. Funções *blockchain* registram uma constatação confiável imutável e rastreável de determinada informação (CARACIOLA, ASSIS, DELLORE, 2019, p. 71).

O *blockchain* opera através da transmissão de informação por meio de chaves criptografadas, que quando efetivada forma um bloco, funcionando de forma semelhante a um livro contábil de registro público, compartilhado e universal (CARACIOLA, ASSIS, DELLORE, 2019, p. 67).

Ao ser adicionada uma informação na cadeia de transações é criado um vínculo com o registro anterior como referência sucessivamente, formando uma cadeia a cada novo bloco distribuída através de vários servidores, não sendo possível alterar qualquer bloco sem que modifiquem os blocos posteriores, de modo a certificar a integridade desses dados de modo eficiente e transparente.

A manutenção decentralizada da base dados garante que qualquer informação entre e saia da rede sem colocar em risco a integridade e a disponibilidade do sistema, visto que todos os usuários são responsáveis por armazenar as informações contidas (CARACIOLA, ASSIS, DELLORE, 2019, p. 68).

Sistemas baseados em funções *blockchain* suficientemente garantem o cumprimento de Desconfiança e Sumidade exigidos para admissibilidade da prova penal. Mas, assim como as demais soluções, se utilizado apenas para certificar a integridade do conteúdo declarado e atribuir uma marca temporal, não se diferem muito de uma certificação qualificada.

Serviços oferecem *blockchain* como garantia de validade jurídica, justamente confundindo certificação de declaração com o conteúdo. A título de exemplo, o PACWEB oferecido pela *OriginalMy* (2021) dispõem que seu serviço “gera um relatório em PDF com dados sobre quem está coletando provas, o *link* para o *post*¸ cópia dos metadados que consistem em importante informação técnica para demonstrar veracidade da prova” (tradução livre do original em inglês).

Através de um *plugin* atrelado ao browser de *internet*, o aplicativo gera um relatório supostamente completo do conteúdo acessado. Alega que garantia de integridade se dá porque o *plugin* recarrega a página acessada, se certificando que modificações impróprias não irão afetar o conteúdo.

A afirmativa ignora que o ambiente virtual de acesso a informações se realiza em várias camadas externas e internas do dispositivo informático. Atrelar a repetição de acesso dentro de um aplicativo demonstra certa ingenuidade o comprometimento com a integridade do conteúdo que o serviço busca vender.

Os metadados que ele se refere sãos os relativos ao dispositivo que acessa a informação, não do conteúdo. Afirma que é coletado o endereço de IP do computador usado para coletar a evidência, o fuso horário e o tempo local, além da geolocalização aproxima, incluindo “muito mais informação”, fazendo inclusive ressalva que há restrição da certificação de fontes privadas de conteúdo, como em mensageiros instantâneos.

Se a informação acessada não teve origem no dispositivo que realiza a captura, os metadados coletados sobre ele não se coaduna com a relevância atribuída pelo serviço.

Soluções digitais são adotadas, mesmo sem regulamentação rígida. “A inércia digital faz com que os Profissionais do Direito esperem que as soluções cheguem prontas, sem que se perceba a potencialidade do momento” (ROSA, 2021, p. 499).

Apesar da referência apresentada se relacionar com a exploração potencial de novas tecnologias para aumentar a performance dos agentes processuais, a remissão aqui se dá em razão da adoção negligente de soluções que lhe são disponibilizadas.

A relevância de tais serviços é defendida recorrentemente como instrumento para coleta segura de prova digital, entrando em meandros na importância da cadeia de custódia e integridade das informações solucionada pelo *blockchain*.

Mas sem qualquer critério do procedimento, pela simples adoção de sistemas que tem potencial apara garantir integridade, acaba retornando aos mesmos problemas relacionados a ata notarial e a certificação digital: garantir a veracidade de uma declaração de conteúdo não equivale a tornar o conteúdo em si verdadeiro.

Condutas realizadas dentro de um sistema de *blockchain* trazem garantia de Sumidade e Desconfiança suficientes para afastar a dúvida sobre sua admissibilidade. Trazer conteúdo externo e declará-lo em um sistema de *blockchain* não transforma o conteúdo em verídico, só assegura a integridade do que foi declarado.

Outra hipótese levantada é quanto ao conteúdo transmitido em tempo real em redes sociais.

A transmissão ao vivo em uma rede social reproduz e arquiva algo que aconteceu em determinado momento. Há quem defenda que, desde que a gravação permaneça disponível para acesso de qualquer interessado, o grau de confiabilidade e impossibilidade de adulteração é elevado, de maneira semelhante a uma ata notarial ou registro em *blockchain* (CARACIOLA, ASSIS, DELLORE, 2019, p. 81).

A razão da atribuição de confiabilidade e impossibilidade de alteração é equivocada, mas a proposta em si de atribuir características de prova concreta não nos parece de todo incorreto.

Os próprios aplicativos permitem a manipulação de imagens por meio de filtros ou equipamentos diversos, além de possibilitar a simples reprodução de registros previamente gravados em uma transmissão ao vivo. Assim, não resta dúvida que há grande possibilidade de adulteração em seu conteúdo.

De outro modo, perfis em redes sociais alcançam *status* notórios de autoria, inclusive algumas plataformas certificando a pessoalidade de alguns em razão disso. Há também a notoriedade adquirida pelo grande volume de acesso de determinados conteúdos, alcançando milhões de pessoas.

Uma mentira contada infinitas vezes não se torna em uma verdade, ao menos pressupondo certo critério à cognição processual penal. Assim, a notoriedade adquirida pelos acessos isoladamente não é relevante no sentido de atribuir veracidade ao conteúdo.

Porém, a notoriedade daquele que disponibiliza não pode ser relevada. Não só aquela relevância atingida dentro das redes sociais, há também canais institucionais oficiais, a título de exemplo do Congresso Nacional e do Poder Judiciário, havendo grau de oficialidade nos conteúdos apresentados.

Os fatos lá documentados teriam notória autoria e seriam testemunhados pelo grande volume de pessoas que vierem acessar, atestando ao menos sua notória existência. A veracidade do conteúdo há de ser objeto do contraditório, mas não restaria dúvidas quanto a pessoalidade e não refutabilidade atribuída documentação do fato lá disponibilizado.

Ainda que seja necessária diligência para conferir ausência de adulterações na representação do conteúdo, algumas especificidades técnicas seriam supridas pela notoriedade, havendo uma presunção dos elementos relacionados a autoria certa e a não refutabilidade de sua existência.

CONCLUSÃO

O proposto modelo garantista de Ferrajoli de processo justo se adequa ao escopo de garantias elencadas no sistema constitucional processual penal brasileiro, sendo possível utilizar seus axiomas para orientar o enfrentamento do tema.

O processo penal condiciona a verificabilidade ou refutabilidade das hipóteses acusatórias a um procedimento de comprovação empírica.

A presunção de inocência enquanto regra de julgamento, exige a legitimidade da atuação estatal dentro da lei, privilegiando a manutenção da liberdade do cidadão quando sopesada a possibilidade de arbítrio indevido de autoridades estatais em sua persecução penal.

O sistema brasileiro é acusatório, havendo por princípio a separação entre órgão de acusação e de julgamento. A acusação não tem poder sobre o acusado, sujeitando suas alegações ao ônus probatório e o contraditório.

A prova é direito subjetivo do acusado, decorrente da ampla defesa conferida pela paridade de armas e a possibilidade de oferecer contraditório. A atividade probatória defensiva contrapõe o ônus acusatório, sendo afeta à administração de risco do acusado em ser condenado.

A possibilidade do juiz produzir prova não é incompatível com a separação da acusação, desde que se limite a produção de meio de prova necessário para incorporar as informações diante da notícia de uma fonte de prova.

Eficiência de um sistema processual penal não é oposto pela previsão de garantias, elas têm função de mitigar riscos não de premiar a impunidade.

Eficiência processual penal não se confunde com a garantia de trunfo da pretensão acusatória, o que equivaleria em reconhecer o procedimento como mera formalidade.

A decisão judicial é uma questão de probabilidade, não de absoluta certeza. A prova tem função de retrospecção, servindo de fundamento para as narrativas processuais e consequente convicção do julgador. O objetivo do processo penal é provocar o juízo a decidir sobre a pretensão acusatória lhe apresentada, confirmando-a ou negando-a.

Através de narrativas processuais se apresentam possibilidades articuladas com as provas disponíveis. Fatos são objetos de prova, enquanto consideração jurídicas sobre eles são objetos argumentação e escolha.

A tipificação penal atribui consequências à realidade, não as narrativas. A incapacidade de cognição absoluta da verdade não impede sua busca e alcance eventual de um grau de certeza.

O grau de certeza alcançado deve ultrapassar a presunção de inocência, obedecendo requisitos de verificação das provas acostadas nos autos.

As regras de exclusão evitam o ingresso de elementos que possam gerar uma reconstrução inexata dos fatos, sendo as provas ilícitas inadmissíveis por previsão constitucional.

O controle epistêmico da prova é realizado para assegurar confiabilidade do que se apresenta. A validade das provas é sujeita ao critério de Sumidade (a prova é exatamente e integralmente aquela que foi colhida) e Desconfiança (é legitimada através de um procedimento que demonstre que a prova é o que se alega que ela é).

Prova digital se refere a qualquer informação preservada em meio digital.

A facilidade de uso de um dispositivo informático oculta sua complexidade. Toda interação é realizada dentro de um ambiente virtual composto por diversos agentes intermediários atuando conjuntamente para realização de tarefas.

A cientificidade da prova pericial é também uma razão de possibilidade, não de verdade absoluta, sendo necessário possibilitar a verificação dos conhecimentos técnicos aplicados.

As informações armazenadas em meio digital têm como características a imaterialidade, volatilidade, fragilidade e dispersão. Seu uso como prova deve considerar tais elementos para garantir o cumprimento dos requisitos de Sumidade e Desconfiança.

A cadeia de custódia tem como função primordial evitar a sujeição da prova a manipulações escusas e erros humanos. Mesmo que não se aplique integralmente os métodos elencados no Código de Processo Penal às provas digitais, a existência de previsão reforça a obrigação de cumpri-la para assegurar a admissibilidade enquanto prova.

A criptografia é um meio de garantir sumidade e integridade de informações. A exploração de vulnerabilidades implica na insegurança de integridade do conteúdo criptografado, visto que o expõem a manipulações.

O regulamento quanto ao uso de criptografia afeta todos os países, ante a natureza global da *internet* e uso universal de aplicativos ofertados nela. Ao mesmo

tempo, restrições de seu uso são pouco eficazes na medida que as práticas criptográficas são amplamente difundidas.

O anonimato é lícito e protegido pela privacidade, não sendo legítimo a vigilância preventiva irrestrita e contínua pelo Estado.

É possível acesso a dados armazenados por provedores de serviços intermediários, tanto os metadados de armazenamento obrigatório quanto aqueles dados que eles armazenam para tratamento em interesse próprio.

Há viabilidade de utilização de *softwares* espiões, porém a exploração de vulnerabilidades prejudica a segurança de integridade dos dados acessados. Seria necessário estipular parâmetros da ferramenta que impedissem a manipulação dos dados e garantissem a auditabilidade do procedimento, com o mínimo de intervenção humana possível.

A busca e apreensão corretamente fundamentada e autorizada judicialmente possibilita a extração de dados armazenados em dispositivos informáticos pela perícia técnica.

Os dados armazenados são sujeitos a serem espoliados ou adulterados. A legitimidade da diligência não impede a prejudicialidade da qualidade das informações acessadas, tanto pelo meio que são coletadas originalmente, quanto pelo procedimento de extração delas.

Vestígios digitais que não obedecem a procedimentos adequados para sua extração ou apresentação deficiente podem ser utilizados na investigação, desde que obtidos por meios legítimos. Se revestem de ilicitude quando apresentados como provas sem a devida diligência.

Ata notarial, certificação digital e funções *blockchain* podem potencialmente ser utilizadas como soluções para garantir sumidade e desconfiança a informações armazenadas em meio digital, desde que utilizadas de modo correto. Certificar a autenticidade de uma declaração não equivale a certificação de integridade e veracidade do conteúdo declarado.

Postas tais conclusões, entende que para o correto uso das provas digitais na conjuntura atual do sistema processual penal brasileiro, é necessário a devida diligência para superar a imaterialidade, volatilidade, fragilidade e dispersão inerentes ao armazenamento digital de informações.

Adentrando o processo como meio de prova sujeito a perícia ou como prova documental, sua admissibilidade é condicionada a garantia de sumidade e

desconfiança através de procedimentos idôneos de extração de dados, obedecendo regras de preservação de cadeias de custódia e possibilitando audibilidade da metodologia e procedimentos adotados, a repetibilidade dos resultados obtidos, a equivalência dos resultados por meio de instrumentos diversos e a justificação dos métodos utilizados para extração, obtenção e processamento dos dados.

De outro modo, encontra problemas de conhecimento técnico por parte dos agentes processuais em sua correta verificação de admissibilidade. Se atribuí elementos errôneos a soluções apresentadas para extração e disposição de informações armazenadas em meio eletrônico, como a confusão entre autenticidade de declarações com a certificação de autenticidade do conteúdo da informação.

Assim, propõe ao fim deste trabalho a necessidade de positivação dos procedimentos de cadeia de custódia no processo penal atinentes a provas digitais, eliminando a dubiedade quanto a aplicação ou não para elas da cadeia de custódia atualmente prevista, com equivalência das etapas de reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento e descartes adequada.

A normatização dos procedimentos adequados ao tratamento da prova digital traria critérios também para utilização de soluções de documentação dos vestígios digitais, visto que as informações necessárias estariam expressas.

Não há maiores problemas ao acesso as informações disponíveis em fontes privadas e públicas de forma legitima dentro da dinâmica normativa à investigação. Há ressalva quanto a exploração de vulnerabilidades de dispositivos informáticos sem a correta regulamentação da ferramenta, porém, a previsão específica de procedimentos de preservação da cadeia de custódia digital orientaria o desenvolvimento de aplicações adequadas, sob pena de serem destituídas de efetividade.

REFERÊNCIAS

ABREU, Jaqueline de Souza; ANTONIALLI, Dennys (eds.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. Vol. I. Ed. Kindle. São Paulo: *Internet* Lab, 2018.

ABREU, Jaqueline de Souza; ANTONIALLI, Dennys. O conto do baú do tesouro: a expansão da vigilância pela evolução e popularização de celulares no Brasil In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. Vol. II. Ed. Kindle. São Paulo: *Internet* Lab, 2019.

ALIMONTI, Veridiana. Criptografia, direitos e a problemática polarização entre "privacidade individual" e "segurança coletiva". In: DONEDA, Danilo; MACHADO, Diego (org.). **A Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 49-67.

ALMEIDA, José Raul Gavião de; FERNANDES, Antonio Scarance; MORAES, Maurício Zanoíde de (Org.). **Provas no Processo Penal**. São Paulo: Saraiva, 2011.

ARANHA, Diego F. O que é criptografia fim a fim e o que devemos fazer a respeito. In: DONEDA, Danilo; MACHADO, Diego (org.). **A Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 23-34.

BADARÓ, Gustavo Henrique. GOMES FILHO, Antônio Magalhães. TORON, Alberto Zacharias. *Coord.* **Código de processo penal comentado**. 2ª ed. São Paulo: Thomson Reuters, 2019.

BADARÓ, Gustavo Henrique. **Epistemologia Judiciária e Prova Penal**. São Paulo: Thomson Reuters Brasil, 2019.

BARBOSA, Daniel Marchionatti; MOURA, Maria Thereza R. de A. Dados digitais: interpretação, busca e apreensão e requisição. In: LUCON, Paulo Henrique dos Santos *et al* (org.). **Direito, Processo e Tecnologia**. São Paulo: Thomson Reuters Brasil, 2020. p. 477-502.

BLUM, Renato Opice; TAMER, Maurício Antonio. Aspectos Processuais da Ação de Quebra de Sigilo para identificação de Responsáveis por ilícitos na *Internet*. In: LUCON, Paulo Henrique dos Santos *et al* (org.). **Direito, Processo e Tecnologia**. São Paulo: Thomson Reuters Brasil, 2020. p. 575-593.

BRASIL. **Constituição da República Federativa do Brasil de 5 de outubro de 1988**. Diário oficial da União, Brasília, 5 de outubro de 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 20 de dezembro de 2020.

_____. **Convenção Interamericana de Direitos Humanos - Decreto nº 678, de 6 de novembro de 1992.** Diário oficial, Brasília, 2 de novembro de 1992. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D0678.htm>. Acesso em 20 de dezembro de 2020.

_____. **Código Penal – Decreto-lei 2.848 de 7 de setembro de 1940**. Diário oficial, Rio de Janeiro, 7 de setembro de 1940. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 20 de dezembro de 2020

_____. **Código Processo Penal – Decreto-lei 3.689 de 03 de outubro de 1941**. Diário oficial, Rio de Janeiro, 13 de outubro de 1941. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em 20 de dezembro de 2020.

_____. **Emenda Constitucional nº 19 de 4 de junho de 1998**. Diário oficial, Brasília, 4 de junho de 1998. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc19.htm>. Acesso em 20 de dezembro de 2020.

_____. **Estatuto da Criança e do Adolescente – Lei nº 8.069 de 13 de julho de 1990**. Diário oficial, Brasília, 13 de julho de 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em 20 de dezembro de 2020.

_____. **Marco Civil da *Internet* – Lei nº 12.965 de 23 abril de 2014.** Diário oficial, Brasília, 23 de abril de 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 20 de dezembro de 2020.

_____. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001.** Diário oficial, Brasília, 24 de agosto de 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em 20 de dezembro de 2020.

_____. **Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709 de 14 de agosto de 2018**. Diário oficial, Brasília, 14 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 20 de dezembro de 2020.

_____. **Lei nº 12.850 de 2 de agosto de 2013**. Diário oficial, Brasília, 2 de agosto de 2013. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em 20 de dezembro de 2020.

_____. Tribunal de Justiça do Rio de Janeiro. Voto Vencido na Apelação nº 0233294-95.2016.8.19.0001. Relator: Desembargador Francisco José de Asevedo. **Diário da Justiça Eletrônico**. Rio de Janeiro. Disponível em: http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=0004C4F922D0D8F90C16A0E8D5294F79937FC5092608331F&USER=. Acesso em: 20 dez. 2020.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 160.662-RJ. Relator: Ministra Aussete Magalhães. Brasília, DF, 18 de fevereiro de 2014. Dje. Brasília.

BUSTAMANTE, Evanilda N. de G. In: BRITO CRUZ, Francisco; FRANGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. Vol. III. Ed. Kindle. São Paulo: *Internet* Lab, 2020. p. 273-292.

CABRAL, Antônio do Passo. Processo e tecnologia: novas tendências. In: LUCON, Paulo Henrique dos Santos *et al* (org.). **Direito, Processo e Tecnologia**. São Paulo: Thomson Reuters Brasil, 2020. p. 83-109.

CARACIOLA, Andrea; ASSIS, Carlos Augusto de; DELLORE, Luiz. Prova produzida por meio de *blockchain* e outros meios tecnológicos: equiparação à ata notarial. In: LUCON, Paulo Henrique dos Santos *et al* (org.). **Direito, Processo e Tecnologia**. São Paulo: Thomson Reuters Brasil, 2020. p. 60-81.

CAMPOS, Francisco. **Exposição de Motivos do Código de Processo Penal.** Decreto-lei 3.689 de outubro de 1941. Rio de Janeiro, 8 de setembro de 1941. Disponível em < https://honoriscausa.weebly.com/uploads/1/7/4/2/17427811/exmcpp_processo_penal .pdf>

CARNELUTTI, Fancesco. **As misérias do Processo Penal**. 3. ed. Leme: Edijur, 2019.

CORREGEDORIA GERAL DE JUSTIÇA DE SÃO PAULO. **Normas de Serviço: Cartórios Extrajudiciais.** Disponível em: https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=133038. Acesso em: 20 nov. 2021.

DEZEM, Guilherme Madeira. **Curso de Processo Penal**. 5ª. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo; MACHADO. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre a anonimização e pseudoanonimização de dados. In: DONEDA, Danilo; MACHADO, Diego (org.). **A Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 137-162.

INTERNET ARCHIVE. **Save Page Now**. Disponível em: https://web.archive.org/save. Acesso em: 3 de novembro de 2021.

FEDERAL AGENCIES DIGITAL GUIDELINES INICIATIVES (Estados Unidos da América). **Term: Digital file**. Disponível em: http://www.digitizationguidelines.gov/term.php?term=digitalfile. Acesso em: 20 dez. 2020.

FERRAJOLI, Luigi. **Direito e Razão**: teoria do garantismo penal. 3. ed. São Paulo: Revista dos Tribunais, 2002.

GUARDIA, Gregório Edoardo Raphael Selingardi. A intervenção nas comunicações eletrônicas e o acesso a dados digitais armazenados em suporte eletrônico como meios de investigação no processo penal. **Revista Fórum de Ciências Criminais - RFCC**, ano 5, n. 5, p. 63-81, jan./ jun. 2016. Disponível em:

https://www.forumconhecimento.com.br/periodico/147/20984/35681. Acesso em: 15 de outubro de 2019.

GUARIENTO, Daniel Bittencourt. MARTINS, Ricardo Maffeis. **Migalhas**. Impressões Digitais: O uso do blockchain na preservação das provas eletrônicas. 22 de maio de 2019. Disponível em: <https://m.migalhas.com.br/coluna/impressoes-digitais/327501/o-uso-do-blockchain-na-preservacao-das-provas-eletronicas?fbclid=iwar0yvdhsa9c3itepugdszrjw9i8y6y62k69mw9saahp6rvip6ty3eksumws>. Acesso em 10 de junho de 2020.

HADJIMATHEOU, Katerina. Vigilância, confiança e a presunção de inocência. In: BRITO CRUZ, Francisco; FRANGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. Vol. III. Ed. Kindle. São Paulo: *Internet* Lab, 2020. p. 18-46.

JORNAL NACIONAL. **Operação Spoofing: PF conclui não ser possível atestar autenticidade e integralidade de mensagens**. Disponível em: https://g1.globo.com/politica/noticia/2021/04/12/operacao-spoofing-pf-conclui-nao-ser-possivel-atestar-autenticidade-e-integralidade-de-mensagens.ghtml. Acesso em: 20 nov. 2021.

KIRO7. **NORWAY to review criminal cases with Danish telecom data**. Copenhagen, 18 de junho de 2019. Disponível em: <https://w,ww.kiro7.com/news/norway-to-probe-criminal-cases-with-danish-telecom-data/980417963>. Acesso em: 24 de setembro de 2019.

LIGURI FILHO, Carlos Augusto. Criptografia em debate: modelos regulatórios ao redor do mundo. In: DONEDA, Danilo; MACHADO, Diego (org.). **A Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 91-106.

LIMA, Renato Brasileiro de. **Legislação criminal especial comentada: volume único**. 4ª ed. Salvador: JusPODIVM, 2016.

LIU, Changwei; SINGHAL, Anoop; WJESEKERA, Duminda. Identifying Evidence for Cloud Forensic Analysis. **Digital Forensics**, Laxenburg, v. 511, n. 12, p. 111-130, 31 ago. 2017. Disponível em: https://link.springer.com/chapter/10.1007%2F978-3-319-67208-3_7#citeas. Acesso em: 20 nov. 2021.

LOPES JÚNIOR, Aury. **Direito processual penal**. 16.ed. São Paulo: Saraiva Educação, 2019.

MÜLLER, Friedrich. **Teoria estruturante do Direito I**. São Paulo: Revista dos Tribunais, 2008.

MANDARINO, Renan Posella. **Limites probatórios da delação premiada frente à verdade no processo penal**. 2016. 270 f. Dissertação (Mestrado) - Curso de Direito, Universidade Estadual Paulista, Franca, 2016. Disponível em: https://repositorio.unesp.br/handle/11449/143920. Acesso em: 20 abr. 2021.

MAGRANI, Eduardo José G.; ABRAHÃO, Luiz. In: DONEDA, Danilo; MACHADO, Diego (org.). **A Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 165-182.

MASSOM, Cleber. **Código Penal Comentado**. 5ªed. São Paulo: Método, 2017.

MENKE, Fabiano. A criptografia e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) In: DONEDA, Danilo; MACHADO, Diego (org.). **A Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 124-136.

NASCIMENTO, Bárbara Luiza Coutinho do. Provas digitais obtidas em fontes abertas na *internet*: conceituação, riscos e oportunidades. In: LUCON, Paulo Henrique dos Santos *et al* (org.). **Direito, Processo e Tecnologia**. São Paulo: Thomson Reuters Brasil, 2020. p. 111-126.

NERES, Winícius Ferraz. A cadeia de custódia dos vestígios digitais sob a ótica da Lei n. 13.964/2019: aspectos teóricos e práticos. **Boletim Científico Esmpu**, Brasília, v. 56, p. 338-382, jun. 2021. Semestral.

NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. **Código de Processo Civil comentado**. 17ª ed. São Paulo: Thomsom Reuters Brasil, 2018.

NETWORK WORKING GROUP. **Guidelines for Evidence Collection and Archiving**. 2002. Disponível em: https://www.ietf.org/rfc/rfc3227. Acesso em: 20 dez. 2020.

NUCCI, Guilherme de Souza. **Curso de Direito Processual Penal**. 17. ed. Rio de Janeiro: Forense, 2020.

OLIVA, Diego Coletti. In: BRITO CRUZ, Francisco; FRANGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. Vol. III. Ed. Kindle. São Paulo: *Internet* Lab, 2020. p. 136-157.

ORIGINALMY. **PACWEB**. Disponível em: https://originalmy.com/pacweb. Acesso em: 3 dez. 2021.

POPPER, Karl. **A miséria do historicismo**. São Paulo: Edusp, 1980.

PRADO, Geraldo. Ainda sobre a quebra da cadeia de custódia das provas. In: **Boletim do IBCCrim**, nº 262, setembro de 2014.

_____. **Prova penal e sistema de controles epistêmicos**. 1ª edição. São Paulo: Marcial Pons, 2014.

_____. Tutela contra a geolocalização contínua. In: BRITO CRUZ, Francisco; FRANGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. Vol. III. Ed. Kindle. São Paulo: *Internet* Lab, 2020. p. 47-63.

PREMIS. **PREMIS Data Dictionary for Preservation Metadata**. 2015. Disponível em: https://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf. Acesso em: 20 dez. 2020.

QUEIROZ, Rafael M. R. Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de troca de mensagens. In: DONEDA, Danilo; MACHADO, Diego (org.). **A Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 35-48.

QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: LUCON, Paulo Henrique dos Santos *et al* (org.). **Direito, Processo e Tecnologia**. São Paulo: Thomson Reuters Brasil, 2020. p. 161-185.

RANGEL, Emanuel Q. Câmeras de segurança e reconhecimento facial: como as imagens são utilizadas como prova no processo penal – notícias do Rio de Janeiro. In: BRITO CRUZ, Francisco; FRANGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. Vol. III. São Paulo: *Internet* Lab, 2020. p. 101-109.

SALVADOR NETTO, Alamiro Velludo. **Tipicidade Penal e Sociedade de Risco**. São Paulo: Quartier Latin, 2006.

SANTOS, Cleopas Isaías Santos; VALE, Samyr Béliche. In: BRITO CRUZ, Francisco; FRANGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. Vol. III. Ed. Kindle. São Paulo: *Internet* Lab, 2020. p. 73-100.

SANTORO, Antônio Eduardo Ramires. A cadeia de custódia na interceptação telefônica. In: CRUZ, Francisco Brito; FRAGOSO, Nathalie (ed.). **Direitos Fundamentais e Processo Penal na Era Digital**: doutrina e prática em debate. São Paulo: *Internet*lab, 2020. p. 244-272.

SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA. **Procedimento Operacional Padrão Perícia Criminal**. Brasília: Ministério da Justiça, 2013. Disponível em: 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: 10 nov. 2020.

ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico**: de acordo com a teoria dos jogos e mcda-a. Florianópolis: Emais, 2021.

TAMER, Maurício; THAMAY; Rennan. **Provas no Direito Digital**. São Paulo: Thomas Reuters, 2020.

TARUFFO, Michele. **Uma simples verdade**: o juiz e a construção de fatos. São Paulo: Marcial Pons, 2016.

TENORIO, Caio Miachon. Anonimato legal na *internet*. In: LUCON, Paulo Henrique dos Santos *et al* (org.). **Direito, Processo e Tecnologia**. São Paulo: Thomson Reuters Brasil, 2020. p. 147-160.

THE LOCAL DENMARK**. Danish police data error may have caused wrong convictions.** Copenhagen, 18 de junho de 2019. Disponível em: <https://www.thelocal.dk/20190618/danish-police-data-error-may-have-caused-wrong-convictions>. Acesso em: 24 de setembro de 2019.

THE INTERCEPT. **Snowden Archive**. Disponível em: https://theintercept.com/collections/snowden-archive/. Acesso em: 20 dez. 2019.

ZANON JUNIOR, Orlando Luiz. GARANTISMO JURÍDICO: o esforço de ferrajoli para o aperfeiçoamento do positivismo jurídico. **Revista da Esmesc**, Florianópolis, v. 22, n. 28, p. 13-38, 2015. Anual. Disponível em: https://revista.esmesc.org.br/re/article/view/119. Acesso em: 01 set. 2021.