A validade do uso da prova digital em nuvem no processo penal

Uma análise crítica ao sistema processual penal vigente sob a ótica da evolução cibernética

Centro Universitário UniCeub - FAJS - Departamento de Direito

Aluno: Augusto de Jesus Fernandes

RA: 2.155.205-7

Sumário

1. RESUMO

Ao longo dos estudos desempenhados buscou-se alocar o maior número de informações relevantes possíveis, mantendo o foco quanto aos temas da era digital e os ramos de atuação do Direito, com principal enfoque às áreas do Direito Penal e Direito Processual Penal, mantendo uma interligação direta com o Direito Informático e o Direito Digital.

A discussão do tema traz as principais questões e "fragilidades", as quais são abordadas na junção das duas esferas temáticas, restando uma abordagem mais teórica e dogmática sobre tais aspectos, tentando aprofundar e visando compreender melhor, os problemas práticos resultantes da defasagem normativa/legislativa, em razão do avanço da tecnologia e do uso rotineiro destes meios. Para definição de parâmetros adequados, os quais delimitaram os termos de realização da pesquisa, foi necessário realizar uma abordagem teórica, passando à uma análise de raciocínio sociológico, e uma interpretação normativo-legislativa dos dispositivos e instrumentos vigentes.

Os recursos metodológicos utilizados foram mais voltados para as discussões teóricas, tendo em vista a relativa novidade temática para os campos de atuação do Direito.

Palavras-chave: Direito Penal. Direito Processual Penal. Prova. Captação. Uso e Validade. Autenticidade e Integralidade. Dados. Interceptação e Quebra. Cadeia de Custódia.Direito Digital. Direito Informático. Digital. Informática. Tecnologia. Inovação. Cibernética. Criptografia. Código. Arquivos de nuvem. *CloudComputing. CloudStorage. Hashing. URL. Backup.* Segurança Digital. Mutabilidade. Volatilidade. Intangibilidade. Manipulabilidade. Anonimidade. Disponibilidade. Confidencialidade. Anomia Legislativa. Omissão. Necessidade de adaptação. Adequação. Princípios do Direito. Presunção de Inocência. Legalidade. Culpabilidade. Jurisprudência. Ausência. Paradigma.

2. INTRODUÇÃO

2.1 Considerações iniciais.

Preliminarmente à uma análise mais aprofundada acerca das problemáticas que envolvem o tema, se faz necessário buscar uma análise dos preceitos e contextos que zoneam cada campo de estudos, tanto pelo aspecto tecnológico quanto pelo aspecto jurídico, o que é desafiador levando em conta a pouca conexão até então existente entre os assuntos levantados por cada um destes ramos de estudo.

Um primeiro olhar deve ser lançado aos aspectos que envolvem o campo da tecnologia da informação, para alcançar um nível mínimo de conhecimento e engajamento no campo a ser abordado, que é o campo das informações, dados e metadados digitais em nuvem, ou o chamado "*Cloud Computing*"[1], para enfim compreender as implicações trazidas ao campo do direito e das relações sociais por essas atividades em nuvem.

Ao passo que se busca fazer a análise destes aspectos da era digital e dos conceitos que envolvem a tecnologia da informação e dos dados digitais em nuvem, é necessário de idêntica forma se atentar à uma perspectiva jurídica mais profunda, voltando-se ao campo do processo penal, e sempre que possível, fazer uma conexão com os mais diversos institutos processuais e procedimentais que envolvem a atuação jurisdicional, principalmente os voltados à utilização destes dados como prova para a persecução penal, buscando vislumbrar os questionamentos, problemas jurídicos e as respostas à eles, que estão sendo trazidos a cada dia por esta realidade da era digital.

2.2 Contextualização histórica e temática.

Para iniciar uma discussão acerca da temática é necessário ter como base certas algumas compreensões históricas e sociais breves, bem como alguns conceitos, com finalidade de viabilizar melhor entendimento no tocante às problemáticas que circundam o atual cenário do Direito e seus campos de atuação em relação aos avanços tecnológicos. Inicialmente faz-se presente a própria explanação das compreensões preliminares quanto às questões históricas em relação à uma contextualização social contemporânea.

---

[1] Terminologia utilizada para computação em dispositivos informáticos em nuvem – **v. cf. OLIVEIRA, Sérgio. Internet das coisas. 2021, p. 90.**

Notavelmente o mundo contemporâneo tem tido evoluções e avanços tecnológicos quase que infindáveis e sucessivos, porém as adaptações sociais em relação a estes fenômenos não vem ocorrendo na mesma proporção, desta forma é compreensível que algumas implicações sociais seriam decorridas deste descompasso; é o que se nota nas cada vez mais constantes invasões de privacidade que vêm se desdobrando no cerne da atual sociedade civil, e aqui se demonstra mero exemplo, mas que detém relevância extrema no campo das relações sociais, consequentemente, de idêntica forma, no campo das relações jurídicas.

É de conhecimento geral que os avanços tecnológicos relacionados à internet e ao uso dela para cometimento de crimes não são nenhuma novidade; ocorre que o descompasso apresentado é advinda de uma conexão intrínseca do uso que o indivíduo dá aos serviços e recursos digitais que estão disponíveis para com suas atividades cotidianas.

Desde a chegada da internet no Brasil, ocorrido em 1988, até a sua regulamentação se passaram quase 30 anos, a qual teve seu marco civil decretado em 2014 através da Lei nº 12.965[2]. Por si só mostra-se que a disparidade entre a normatização e o uso em si, nas ocasiões de mundo fático, iriam em algum momento trazer consequências voltadas à própria atividade estatal punitiva, e o que antes era uma mera mudança de cotidiano social acabou por se desenrolar em inúmeros fatos antijurídicos, demandando assim muito mais do aparato estatal e do próprio ordenamento jurídico para se fazer valer frente àqueles gerados.

Mas ainda que uma atuação normativa mais contumaz venha a ocorrer no cenário contemporâneo sempre será necessária uma adaptação sucessiva e constante deste contexto normativo, assim como também do aparato estrutural e funcional ligado à ele, aqui já se falando de recurso humano, o qual se valerá desta norma para fazer cumprir a regulamentação compatível e existente, quando esta houver.

Em um segundo momento, é feita uma abordagem destes conceitos. É imprescindível ter um foco mais detalhado para os ramos do Direito Digital e Direito Informático e sua recente interdisciplinaridade estrita com o Direito Penal e Direito Processual Penal; dito isto, preliminarmente, quanto aos aspectos jurídicos, se discute o conceito de instrumentos processuais tais como o de prova, de cadeia de custódia, de investigação policial, de investigação na seara digital, de procedimento investigativo, de perícia, de nulidade processual e procedimental, do devido processo legal, do contraditório e da ampla defesa, de violação a princípios processuais, etc.

[2] Institui a Lei do Marco Civil da Internet no Brasil – **v. cf. Lei n[3] HASSAN, Nihad A. Perícia Forense Digital. 2019.**

Serão identicamente abordados os aspectos técnico-científicos relacionados aos dados digitais e aos sistemas informativos de dados digitais; os diferentes métodos utilizados para gerir estes dados e sistemas; as características de cada um deles; as técnicas empregadas para análise de cada um deles; a compreensão de quais dados são necessários e imprescindíveis para a compreensão de determinada informação digital.

Em seguida serão apresentados os aspectos processuais voltados à uma óptica dos ramos do Direito Penal; a atuação estatal frente os processos penais em andamento; as técnicas, métodos e procedimentos empregados nos processos penais em curso; a legislação vigente e a delimitação dos conceitos e abrangência nela contida; as práticas utilizadas com relação aos processos em andamento frente à esta legislação; a perspectiva de diversos ângulos possíveis sobre as limitações trazidas pela legislação vigente.

De idêntica forma são explanados conceitos sobre crimes em espécie, com principal enfoque aos crimes cibernéticos, neste momento já voltados aos instrumentos do direito material na esfera penal, assim como também preceitos e princípios do direito processual penal; posteriormente faz-se a mesma abordagem de tema, mas neste momento voltados ao Direito Digital e Direito Informático, em específico quanto aos conceitos de prova digital, de cadeia de custódia digital, de investigação cibernética, de perícia digital, de análise criptográfica, de prova digital em nuvem, meio de obtenção da prova digital, etc.

À posteriori será feita uma análise crítica aos olhos da junção dos elementos técnico-científicos apresentados frente às questões processuais também suscitadas, de modo a abranger a discussão tanto pela ótica estatal para exercício dos seus poderes, quanto pelo ponto de vista da liberdade do indivíduo que eventualmente sofrerá reprimendas estatais decorrentes da atividade estatal e exercício destes poderes.

Por fim, é feita uma análise crítica acerca das implicações e questões problemáticas trazidas por este quadro apresentado em detrimento do sistema penal e processual penal vigente, levando em conta aspectos legislativos, aspectos sociais, aspectos constitucionais, aspectos normativos, aspectos jurisprudenciais e doutrinários, até mesmo alguns argumentos trazidos do direito comparado, tudo isto com a finalidade de viabilizar uma melhor discussão nas rodas que são e continuarão sendo afetadas por estes questionamentos e problemas, e visando a busca de soluções cabíveis e compatíveis ou o mais próximo possível disto.

Os principais dilemas a serem enfrentados no debate exposto estão diretamente interligados ao fundamento de inovação técnica para os campos de atuação, bem como a ausência de instrumentos e aparatos estatais, os quais tornem hábeis e viáveis a regulamentação adequada, da devida utilização procedimental, destes meios tecnológicos, principalmente se

voltados às questões ligadas ao uso desses para processos criminais, os quais tratam da liberdade do indivíduo.

Questões problemáticas relacionadas à violação de direitos fundamentais; situações de investigações fragilizadas, principalmente em detrimento do aparato estatal defasado para realizar tal atuação; ocasiões de impunidade, em razão de atividade estatal ineficaz e incompatível com as constantes mudanças na seara tecnológica; desamparo legislativo para certas condutas que ainda não tem previsão legal; atuação estatal ineficiente dos poderes em geral, em especial para com o Poder Judiciário, com aplicação de eventuais entendimentos jurisprudenciais incondizentes com a realidade fática, bem como arbitrariedades diversas.

3. Conceituação e análise técnica.

Foram utilizadas abordagens acerca das diferentes perspectivas técnicas que envolvem a temática, tanto pelo aspecto tecnológico quanto pelo aspecto jurídico e normativo, de modo a distinguir a atuação procedimental em circunstâncias mais rotineiras e já anteriormente normatizadas, com posicionamento firmado na jurisprudência, daquelas mais surpreendentes e inovadoras ao sistema jurídico processual vigente, ainda mais no que tange ao Processo Penal.

É sabido que o movimento progressista, acerca da globalização e informatização através dos meios de comunicação digitais, está em cada vez maior constância, enquanto que a atuação dos profissionais e técnicos nas respectivas áreas, acaba por ficar defasada em relação aos avanços contemporâneos apresentados, ainda mais no que se relaciona com as técnicas e procedimentos empenhados ao longo do Processo Penal, em principal para com os relacionados diretamente com as provas digitais e a cadeia de custódia digital; deste modo, não podem se eximir os campos de atuação da regulação social, que é feita através da norma e da sua devida aplicação, de efetuar esta respectiva análise e enfrentamento da questão.

Tendo em vista esta necessidade, bem como da sua respectiva normatização, apesar de serem poucas as correntes teóricas na doutrina pátria que o debatem, vêm ocorrendo uma mobilização para se discutir acerca das possibilidades e de que forma isto seria realizado, abordando os diferentes critérios a serem utilizados, assim como também a viabilidade de implementação destas possibilidades.

Houve aprofundamento quanto ao tema quando realizada uma interpretação dos textos de Nihad A. Hassan[3], de Jonathan Weber[4], Sérgio de Oliveira[5], Bill Gardner[6] e outros, os quais tratam justamente dos aspectos tecnológicos e das respectivas conceituações e definições informativas, necessárias para discussão do que se trataria de uma verdadeira atuação em procedimento de perícia forense digital[7], ainda mais no que diz respeito à devida observância aos critérios técnicos, relacionados com a natureza dos dados e metadados digitais[8], bem como de termos como *Cloudcomputing*[9] e *Cloudstorage*[10], os quais são objeto dos devidos procedimentos jurídicos e investigativos, com finalidade de serem utilizados ao longo dos processos criminais.

Já no tocante à discussão temática voltada aos conhecimentos, conceitos e aspectos principiológicos basilares dos ramos de atuação jurídicas, estes foram abordados com melhor ênfase quando analisados os textos de Guilherme de Souza Nucci[11], Aury Lopes Júnior[12], e Renato Brasileiro de Lima[13], os quais trazem as noções mínimas para se viabilizar a conexão temática entre os aspectos da Tecnologia da Informação e o Direito, principalmente o Direito Penal e o Direito Processual Penal; aqui se encontra o momento de conjuntura entre a ideologia de Cadeia de Custódia[14], de Prova[15], de Procedimento[16], de Investigação[17], de Ampla Defesa e Nulidade Processual[18], dentre outros conceitos do Direito, para com as primeiras noções problemáticas relacionadas ao avanço da tecnologia e as regulações sociais.

Quanto à intrínseca ligação entre os ramos do Direito Informático com o Direito Penal e Direito Processual Penal, bem como as implicações sociais trazidas pelos ramos da Tecnologia da Informação, aqui já se realizando um aglomerado maior de informações basilares e também mais específicas, foram utilizados os estudos de Spencer Toth Sydow[19], o qual faz uma bela explanação das situações problemas, bem como das diferentes perspectivas teóricas que já estão em andamento, ou que ainda devem surgir em relação à eles.

---

[3] **HASSAN, Nihad A. Perícia Forense Digital. 2019.**
[4] **WEBER, Jonathan. Google Analytics e Google Tag Manager para Desenvolvedores. 2016.**
[5] **OLIVEIRA, Sérgio. Internet das coisas. 2ed. 2021.**
[6] **GARDNER, Bill; LONG, Johnny; BROWN, Justin. Google Hacking para Pentest. 1ed. reimp. 2018.**
[7] Conceito trazido para a análise pericial de dados e metadados digitais – **v. cf. HASSAN, 2019, p. 21.**
[8] Conceitos trazidos para definição da terminologia dos dados e metadados digitais – **v. cf. ARARAKI; ARARAKI. 2021, p. 37.**
[9] Terminologia utilizada para computação em dispositivos informáticos em nuvem – **v. cf. OLIVEIRA, 2021, p. 90.**
[10] Terminologia utilizada pela Tecnologia da Informação – **v. cf. SYDOW, 2022, p. 77.**
[11] **NUCCI, Guilherme Souza. Leis Penais e Processuais Penais Comentadas - Vol. 1. 14ed. 2021.**
[12] **JUNIOR, Aury Lopes. Direito Processual Penal. 20ed. 2023.**
[13] **LIMA, Renato Brasileiro. Manual de Processo Penal - vol. único. 10ed. 2021**
[14] Conceito trazido pelos ramos do Direito Processual Penal – **v. cf. JUNIOR, 2023, p. 481.**
[15] Conceito trazido pelos ramos do Direito Processual Penal – **v. cf. NUCCI, 2022, p. 29-30.**
[16] Conceito trazido pelos ramos do Direito Processual Penal – **v. cf. JUNIOR, 2023, p. 871.**
[17] **Opus cit. p. 107.**
[18] **Opus cit. p. 81-82.**
[19] **SYDOW, Spencer Toth. Curso de Direito Penal Informático. 3ed. 2022.**

De igual forma, tem-se de base os estudos de Sérgio Ricardo de Souza[20], Rennan Thamay e Maurício Tamer[21], em conjunto com os estudos de Hassan, onde se explana muito acerca do raciocínio final necessário para o tema, que é justamente a idéia de desenvolvimento inicial de uma "cadeia de custódia digital" e da utilização dos devidos procedimentos forenses[22], para implementação e viabilidade da utilização de dados e metadados digitais em nuvem, como meios de prova no processo criminal.

3.1 Os aspectos que envolvem os dados digitais - conceitos e características.

O primeiro conceito a ser abordado, para o melhor entendimento sobre as questões contidas no campo da tecnologia da informação e do uso de dados digitais, é a figura dos metadados de arquivos digitais.

Hassan[23] conceitua os metadados como sendo dados sobre dados, e explica que "Os metadados contém dados que descrevem os arquivos aos quais estão associados[...]", fazendo assim com que um grupo de dados digitais possam ser compartilhados entre indivíduos conforme sua referenciação direta esteja relacionada a determinado arquivo, de modo que um determinado indivíduo ao receber a informação de outro, poderá saber a qual arquivo aquele determinado dado está se referindo. Deste modo, indivíduos de qualquer parte do globo podem trocar informações entre si, sabendo sobre o que o emissor da informação estará enviando e sobre o que se trata.

O próximo passo necessário para a compreensão de como funcionam as trocas de informações no ambiente digital é a explanação do conceito de endereço de IP[24]; o endereço de IP é um meio de realização de protocolo que possibilita a obtenção da destinação de uma determinada mensagem ou metadado digital. É o meio pelo qual se possibilita uma conexão virtual de determinado aparelho eletrônico com outro, de modo a definir um esquema de emissor-destinatário, podendo ser realizado através de uma conexão privada ou não.

Vale realizar a ressalva quanto aos procedimentos de camuflagem de endereço IP, bem como as práticas antiforense digitais[25], as quais são utilizadas como mecanismo de entrave à identificação direta e concisa do dispositivo eletrônico específico que realizou determinado comando digital, visando esconder a identidade do usuário do dispositivo, que pode estar se valendo desse meio para prática de atividades ilícitas, mas tal discussão será melhor abordada posteriormente.

---

[20] **SOUZA, Sérgio Ricardo. Prova Penal e Tecnologia. 2020.**
[21] **THAMAY, Rennan; TAMER, Maurício. Provas no Direito Digital. 2ed. 2022.**
[22] **Procedimento forense digital – v. HASSAN, Nihad A. Perícia Forense Digital. 2019.**
[23] Opus Cit. p. 59
[24] Opus Cit. p. 78.
[25] Opus Cit. p. 262-263.

Hassan[26], explica que os endereços de IP podem se assemelhar a uma impressão digital eletrônica, não podendo existir mais de um endereço de IP igual na mesma rede de IP; desta forma pode-se delimitar especificamente de qual aparelho eletrônico está sendo enviada determinada informação, dado ou metadado e exercendo determinada comunicação, através de apuração de qual o endereço eletrônico que está sendo utilizado na troca de determinado dado ou metadado digital. É o que se afirma (*sic)*:

> [...]
> Normalmente o IP é associado a outro protocolo chamado Transmission Control Protocol (TCP), o qual permite que o dispositivo de computação estabeleça uma conexão virtual entre um destino e uma origem para trocar informações. (HASSAN, 2019, p. 78).
> [...]

Na mesma linha, Oliveira[27] afirma que "[...] todas (ou quase todas) as aplicações de modelos TCP/IP usam o modelo de comunicação cliente/servidor", o que acaba por gerar uma confiabilidade ao menos de que se trata de uma troca de informações entre os aparelhos eletrônicos X e Y contidos em uma determinada rede de IP's, seja esta uma rede pública ou privada.

Porém, para se obter ciência acerca da utilização de determinado endereço de IP conectado à uma rede privada, será necessário a realização de uma etapa extra de identificação, preliminarmente à obtenção do próprio IP, sendo esta a verificação do provedor de conexão de rede utilizado pelo usuário do dispositivo eletrônico ao qual pertence o IP buscado. O provedor de conexão de rede[28] são os responsáveis pelo fornecimento de determinado endereço eletrônico de IP para determinado dispositivo eletrônico conectado à internet, de modo a gerar determinado código para determinado dispositivo sem sobrecarregar a rede mundial de internet, e trazendo uma possibilidade de identificação daquele determinado dispositivo por meio de seu IP.

Ainda que se ultrapasse a discussão acerca do endereço de IP, tem de ser levantadas as informações do provedor de rede, com finalidade de afunilar a busca no procedimento investigativo, visando alcançar a situação de nexo causal entre o delito cometido e os dispositivos eletrônicos envolvidos.

Além disto, tem-se que, apesar de se delimitar com precisão e especificidade quais os aparelhos eletrônicos que estão envolvidos em determinada troca de informações, dados ou metadados, tal inferência não é suficiente para delimitar quem estava no uso daquele

[26] **HASSAN, 2019, p. 78.**
[27] **OLIVEIRA, 2021, p. 22.**
[28] Explanação realizada sobre o que chega a ser um provedor de conexão de rede – **v. cf. ELEUTÉRIO; MACHADO. 2019, p. 108.**

determinado dispositivo, naquele determinado momento e sob quais condições e finalidades estava se transmitindo determinada informação, dado ou metadado; ainda restará saber com exatidão quem é o indivíduo por trás do aparelho eletrônico que emanou o comando. Aqui residem as criticas jurídicas pertinentes em tópico próprio.

Seguindo este entendimento, faz-se necessário o uso de mecanismos para atingir um nível de certeza quanto ao indivíduo que esteja se valendo do uso de determinado dispositivo eletrônico naquele determinado momento, como é o caso de uso de camadas digitalizadas de autenticação do usuário[29], o que acabaria por sanar a problemática da incerteza quanto ao usuário que estaria ou não na posse de determinado aparelho eletrônico.

Algumas destas ferramentas já são utilizadas por grande parte das empresas de produção em massa de meios de tecnologia da informação e de transmissão de dados digitais, como são os exemplos das autenticações de dois ou mais fatores[30], que nada mais são do que diferentes métodos de autenticação, com emprego de diferentes procedimentos distintos, mas vinculados e concatenados entre si, que ao concretizar uma etapa de autenticação passa-se para a próxima, até que se concluam todas as etapas do processo de forma correta, dando assim ensejo a "integridade e certeza" do domínio de determinado indivíduo sobre determinado dispositivo naquele determinado momento.

Nota-se a importância da conclusão concisa de cada uma destas etapas, a fim de possibilitar uma identificação concreta do agente que está se valendo do meio digital para realizar a prática de determinado ato no mundo dos fatos.

Ora, aqui passa-se a ter uma identificação mais clara sobre a chamada "cadeia de custódia da prova digital" e a sua importância nos processos de natureza penal, principalmente no tocante ao uso de informações e dados digitais para possibilitar o exercício do poder punitivo estatal de forma adequada e coerente. Mas aqui se trata de análise de aspectos técnico-jurídicos, que abordam as questões processuais e procedimentais do uso de dados digitais e da investigação forense digital, que passará a ser abordada com mais ênfase à posteriori.

Por fim é preciso compreender que as etapas de autenticação acabam por passar por sistemas integrados de comunicação, que são as chamadas "camadas de rede digitais"[31], mas para melhor entendimento sobre o que são e o modo de funcionamento destas é necessário a

---

[29] Sydow faz o comparativo entre uma arma e um dispositivo eletrônico, para tentar figurar a ideia de incerteza quanto à autenticidade da pessoa, no que se referem à elementos de autoria do momento do cometimento do ilícito. Fenômeno chamado de "IMPRECISÃO DE AUTORIA" por Sydow – **v. cf. SYDOW, p. 118.**

[30] *Multiple steps verification procedures* - **v. cf. SYDOW, 2022, p. 119**.

[31] Conceito trazido pelos ramos da Tecnologia da Informação, voltadas às atividades da Perícia Forense Digital – **v. cf. OLIVEIRA. 2021, p. 24.**

disposição de conceitos sobre os microprocessadores[32] e microcontroladores[33] que compõe parte dos sistemas das "interfaces digitais"[34].

Os microprocessadores são pequenos componentes físicos de um aparelho eletrônico, que acabam por fazer parte de um componente maior, que são os chips de processador daquele aparelho, que é responsável pela capacidade daquele determinado dispositivo eletrônico elaborar e processar determinada informação, dado ou metadado digital; sendo assim, os microprocessadores compõem a CPU de um determinado aparelho eletrônico, conforme explica (*sic*):

> [...]
> Assim como a densidade dos elementos nos chips de memória continuava a subir, a densidade dos elementos dos chips do processador também subia. Com o passar do tempo, mais e mais elementos eram colocados em cada chip, de modo que menos e menos chips eram necessários para se construir um único processador do computador.
> [...]
> Uma descoberta inovadora foi alcançada em 1971, quando a Intel desenvolveu seu 4004. Ele foi o primeiro chip a conter em si todos os componentes de uma CPU em um único chip: nascia o microprocessador. (STALLINGS, 2017, p. 21).
> [...]

Já os microcontroladores são também componentes de um determinado aparelho eletrônico, porém são destinados a executar tarefas de forma autônoma e sem a interação humana, como método de inclusão de outras mais tarefas no mesmo componente, de modo que este acabe por gerar as portas de entrada e saída de determinado comando digital. Conforme se explica:

> [...]
> Alguns desses componentes começaram a se destacar na automatização dos dispositivos e sistemas por agregar mais funcionalidades no próprio componente, recebendo o nome de SoC (*System-on-Chip*). Dispositivos com essas características começaram a ser chamados de microcontroladores devido ao seu uso na função de controle e automação.
> Os microcontroladores têm interface de entrada e saída com dispositivos elétricos como botoeiras e relés (OLIVEIRA, 2021, p. 45)
> [...]

Da mesma forma Stallings[35] afirma que "O microcontrolador é programado para uma tarefa específica, embarcada em seu dispositivo, e executa como e quando necessário". Deste modo, um microcontrolador irá desencadear os componentes de entrada e saída de

---

[32] Conceito trazido pelos ramos da Tecnologia da Informação – **v. cf. STALLINGS, 2017, p. 21.**
[33] Conceito trazido pelos ramos da Tecnologia da Informação – **v. cf. OLIVEIRA. 2021, p. 45.**
[34] Opus Cit.
[35] **STALLINGS, 2017, p. 45.**

determinadas informações, dados ou metadados de um determinado dispositivo eletrônico, que serão realizados através das "interfaces digitais"[36].

Criada a porta geradora de entrada e saída de determinada informação, dado ou metadado, será realizada a transmissão destes de forma a garantir o sistema de redes de informação que está sendo utilizada naquela determinada transmissão, podendo assim se identificar também por consequência os dispositivos eletrônicos que estão ligados àquela determinada rede, naquele determinado momento, transmitindo aquela determinada informação.

Além das informações acerca dos dispositivos eletrônicos e seus componentes, bem como de seu funcionamento, há também de ser levada em conta ocasião diretamente interligada aos dados digitais em nuvem, os quais consistem na disponibilização de arquivos, contidos em dispositivos eletrônicos físicos, em meios e mecanismos de rede através de bancos de dados[37] digitalizados e virtualizados, os quais têm seu acesso facilitado para aqueles que sabem onde se encontra àquela determinada informação, podendo alcançá-las, depositá-las, armazená-las, distribuí-las, disponibilizá-las, modificá-las e até mesmo gerí-las em através de qualquer dispositivo eletrônico no mundo, devido sua procedimentalização específica, que acaba por retirar a "rastreabilidade" do aparelho ou dispositivo eletrônico o qual o disponibilizou.

Algumas considerações devem ser levantadas ao abordar os aspectos tecnológicos, bem como os conceitos técnico-científicos que envolvem o termo "*Cloud Computing*"[38]. A terminologia é utilizada para a utilização de serviços digitais informativos, através de sistemas que descentralizam a rede, de modo a possibilitar o acesso dos serviços e dados digitais através de qualquer dispositivo, em qualquer lugar, apenas se valendo daquela rede descentralizada de informações que se encontra solta em um localizador digital contido na internet, o qual antes de sua disponibilização em rede descentralizada se encontrava em dispositivo eletrônico físico e rastreável.

É o mesmo que se valer de um departamento de arquivologia digitalizada, aqui já se voltando ao termo "*Cloud Storage*"[39], utilizando de servidores externos, em um sistema que não seja fisicamente acessível, nem tampouco pode ser resguardado em um único dispositivo ou aparelho eletrônico; é a possibilidade de uso de conexão àquela determinada rede através de quaisquer meios eletrônicos disponíveis ao usuário. Conforme se expressa:

[...]

---

[36] Oliveira traz as conceituações de interfaces de rede e seus subtipos, bem como funcionalidades – **v. cf. OLIVEIRA, 2021, p. 47-49.**
[37] **OLIVEIRA, 2021, p. 93.**
[38] Opus Cit. p. 90.
[39] **SYDOW, 2022, p. 76.**

> Esta é a computação na nuvem. O uso da conexão à rede e o processamento dos navegadores para dar ao usuário acesso a programas e arquivos sem que ele precise instalar ou manter dados em sua máquina de modo cumulativo e exaustivo. (SYDOW, 2022, p. 71).
> [...]

Esta situação de armazenamento de informações, dados e metadados digitais em servidores externos de rede, tem consigo algumas características que estão diretamente interligadas ao funcionamento destes sistemas de nuvem, em principal destaque à ausência de necessidade quanto à capacidade de armazenamento de determinadas informações e dados digitais; é o que Oliveira[40] afirma "Se esse elemento estiver na nuvem, as aplicações ganham mais flexibilidade e escalabilidade. Além disso, evitam a necessidade de um servidor de alta disponibilidade".

A situação da constante inovação tecnológica, juntamente com a adaptação tardia dos profissionais pertencentes aos ramos da tecnologia da informação, acabando por precarizar alguns dos serviços prestados, sendo necessária a idêntica evolução e adaptação daqueles operadores destes ramos, levando assim à situação de atividade forense digital voltada à estas especificidades trazidas pela informatização em sistemas de nuvem.

Juntamente com as terminologias "*Cloud Computing*" e "*Cloud Storage*" vieram as inovações no campo do armazenamento de dados digitais, e com elas vieram também as implicações para aqueles que se utilizam destes meios para realizar o cometimento de fenômenos antijurídicos, se valendo também destes mecanismos digitais para acabar mascarando ou apagando as evidências contidas naquelas informações ou dados digitais.

3.1.1 As características inerentes aos dados digitais.

É necessário compreender até mesmo o raciocínio originário por trás da problemática inerente ao uso dos dados digitais, para que se possa entender também os encadeamentos que tal realidade factual pode trazer ao mundo jurídico, principalmente quanto à aplicabilidade das normas, o modo como será feita a tomada de decisão baseada nestas normas, como tal raciocínio irá afetar a esfera jurídica, bem como as limitações que devem ser impostas às situações cotidianas e até mesmo as possíveis implicações legislativas.

Deve ser ressaltada, aos olhos de parte da doutrina que trata do tema, que as inovações tecnológicas trazem consigo implicações próprias, de modo que sejam debatidos e

[40] **OLIVEIRA, 2021, p. 91.**

demonstrados os pontos relativos às próprias características inerentes aos dados digitais, levando em conta a maleabilidade, volatilidade e mutabilidade de dados, conforme se demonstra:

> [...]
> A partir de nossos estudos concluímos que são 16 (dezesseis) as características da delinquência informática: 1) a interatividade ou comando, 2) a mobilidade, 3) a conversabilidade, 4) a conectividade, 5) a mundialização, 6) a ubiquidade, 7) a fracionabilidade, 8) a divisibilidade, 9) a intangibilidade, 10) a disponibilidade, 11) a pluralidade, 12) a velocidade, 13) a não territorialidade, 14) manipulabilidade, 15) anonimidade e 16) inevitabilidade. (SYDOW, 2022, p. 280-281).
> [...]

De igual maneira o pensamento se expõe em:

> [...]
> As principais características das mídias de armazenamento digitais, de interesse à Computação Forense, são: fragilidade, facilidade de cópia, sensibilidade ao tempo de vida e sensibilidade ao tempo de uso. (ELEUTÉRIO; MACHADO, 2019, p. 51).
> [...]

Tais características infirmam claramente a situação de risco ao se utilizar de dados e metadados digitais como meio de prova para com os processos criminais em curso, isto pois cada uma dessas traz aspectos altamente instáveis, podendo a qualquer tempo serem corrompidas as tais provas decorridas da utilização desses dados e metadados digitais. Tamanha incerteza, ao se valer de tal prova no curso de uma instrução criminal, se reveste de uma clara maculação da referida instrução, é o que se nota:

> [...]
> Há possibilidade de perda de dados. Ainda que haja segurança no armazenamento de dados, é possível que, na transmissão, por questões técnicas, ou mesmo por sabotagem, os dados sejam perdidos, modificados ou destruídos e o usuário não guarde seus *backup*, confiando no serviço. (SYDOW, 2022, p. 79).
> [...]

Deve-se levar ainda em consideração que a realidade fática da sociedade é a inovação tecnológica constante e desenfreada, e que tal velocidade de avanços tecnológicos se mostra pela natureza humana insaciável de se sentir na necessidade de constante evolução, juntamente com uma parcela de luxo social, implementada pela idêntica natureza humana de consumir, que acabam por trazer ciclos infindáveis de reinventar as situações cotidianas da vida.

Exemplo claro disto é o fato de que hoje se tem até mesmo as chamadas "nuvens de armazenamento de dados", também chamadas de "*cloud computing"* e "*cloud storage"*, tamanha a evolução dos sistemas de informação que se tem nas situações factuais da atualidade.

Tais sistemas de armazenamento de dados se mostram verdadeiras ferramentas de "fragilidade probatória", frente às normas atualmente vigentes para regulação da utilização de provas contidas nestas "nuvens", isto porque ao consumir um produto com esta disposição o usuário não tem controle sobre nenhuma das características desta, veja-se:

> [...]
> Há, assim, uma sensação de independência da localização posto que o consumidor não possui poder de decisão, controle ou conhecimento sobre o exato local dos recursos do provedor - podendo conhecer genericamente o local do *datacenter* onde estão os dispositivos. (SYDOW, 2022, p. 76).
> [...]

Ocorre assim uma problemática frente à atuação do poder público estatal, que está atrelada a fragilidade inerente à própria função e usabilidade dos dados digitais, e aqui valem ser ressaltadas as consequências do uso de dados digitais, tendo em vista as suas características inerentes. Desta forma demonstra que:

> [...]
> Da mesma forma, do ponto de vista normativo, tanto os trabalhos de observação, de caráter exploratório, analítico ou empírico, quanto aqueles propositivos partem, por exemplo, de experiências comparadas sobre as formas pelas quais o direito, com suas construções teóricas, doutrinárias e narrativas, enfrenta a natureza polissêmica das tecnologias: órgãos legislativos, executivos e judiciais devem manter diálogos com aspectos técnicos, políticos, econômicos e sociais implicados nos segmentos tecnológicos ao redor do globo, confrontando-os com os distintos países e seus sistemas jurídicos. Isso porque entre as principais características dos bens tecnológicos e informacionais está sua inequívoca mobilidade além-fronteiras. (POLIDO; BRANDÃO; ROSINA, 2019, p. 396).
> [...]

Aqui deve ser realizada uma nota adicional quanto à estas características, tendo em conta principalmente os aspectos interligados com a mutabilidade de dados, a sua volatilidade[41] e extensa fragilidade, sua manipulabilidade, as quais trazem toda a situação de instabilidade quanto ao seu uso no curso das investigações criminais conduzidas, bem como outras características tais como a intangibilidade[42], a conectividade[43], a anonimidade[44], as quais demonstram a difícil interligação com um sujeito determinado, de modo a ser capaz de cumprir com os requisitos objetivos da norma para realizar a referida instrução criminal.

Analisando as citadas primeiras características, que trazem a instabilidade levantada, tem-se que a mutabilidade está diretamente relacionada com a possibilidade de realização de práticas antiforenses, no intuito de obstruir o acesso à íntegra de dados, ou de até mesmo editar

[41] Neste sentido são trazidas as características de volatilidade da prova digital – **v. cf. PITTIRUTI, 2011, p. 11.**
[42] Características trazidas pela doutrina que trata do Direito Digital e Informático – v. cf. **SYDOW, 2022, p. 299.**
[43] **Opus cit. p. 287.**
[44] **Opus cit. p. 311-312.**

o seu conteúdo, visando desconstituir as provas de eventual fenômeno antijurídico, através de manipulações sucessivas de determinado dado ou metadado digital, de modo a inviabilizar a identificação da verdade real por trás daquele determinado dado, esta que é um princípio norteador do processo penal. Este é o exato pensamento prelúdio quanto à manipulabilidade, veja:

> [...]
>
> Tudo que compõe uma relação informática pode ser manipulado: os elementos que apontam para autoria, os elementos de materialidade, a legitimidade da conexão, arquivos podem ser manipulados de modo a violar sua integridade ou sua disponibilidade, senhas podem ser manipuladas para dar acesso a sistemas e programas sem autorização legal do legitimado entre tantos elementos.
> [...]
>
> Ou seja, praticamente todos os elementos informáticos com os quais lidamos no dia a dia são sujeitos a mudanças que podem servir de legitimação para condutas delituosas ou para incriminações indevidas. Aqui, as *deep fakes*, as montagens, o uso de inteligência artificial e a necessidade de autenticação a partir de ferramentas como a Verifact. (SYDOW, 2022, p. 310-311).
> [...]

Já no tocante aos aspectos ligados à volatilidade e a extensa fragilidade dos dados e metadados digitais, deve ser enaltecida a sua conexão com a chamada evidência digital[45], que será abordada mais profundamente em subtópico específico adiante, de modo a trazer levantamentos necessários quanto à integridade dessas evidências para que tenham posteriormente sua finalidade convertida em definitivo para status de prova digital. Veja que tal compreensão é claramente demonstrada: *sic*

> [...]
>
> Na etapa de priorização entre coleta ou aquisição de uma evidência digital é fundamental que o agente entenda todas as circunstâncias para coletar ou adquirir a potencial evidência digital. Entretanto, pode ser necessário priorizar itens pela volatilidade e/ou pelo valor probatório quanto a sua relevância. Itens de valor probatório de alta relevância são aqueles que são mais prováveis de conter dados relativos diretamente ao incidente investigado.
>
> A evidência digital pode ser dividida em duas categorias:
>
> *Dados* voláteis ou Dados não voláteis, estas definições são aplicadas às memórias (componentes de armazenamento de informações). A memória RAM é considerada um tipo de memória "volátil", pois todos os dados que não forem guardados de forma permanente serão apagados após desligamento do computador. A memória ROM e os outros dispositivos de armazenamento de dados são considerados "não voláteis" (pendrive, HD, SDCard, etc)
>
> Após a identificação, é recomendado ao agente:

[45] Conceito trazido pelos ramos da Tecnologia da Informação, em especial pelas áreas da Perícia Forense Digital – **v. cf. HASSAN, 2019, p. 35-36.**

> - Priorizar a potencial evidência digital que pode ser perdida para sempre se a fonte de energia for removida; e
> - Tomar ações rápidas para adquirir este dado utilizando métodos validados.
>
> Obs: Quando há suspeita de criptografia ou de um programa malicioso, será necessário adquirir o dado volátil. (OLIVEIRA, 2018).[46]
> [...]

Passando-se assim para a característica da mutabilidade, fica claro que a ocasião de fácil alterabilidade dos dados e das informações nele contidas trazem uma grande preocupação para as autoridades investigativas, as quais se valerão destes dados para conduzir seus esforços na busca da evidência digital, principalmente quanto ao seu aproveitamento de uso como real evidência. Daniele[47] se refere a isto como sendo "uma característica de mutabilidade congênita" dos dados digitais, os quais claramente influenciam na devida procedimentalização por parte dos profissionais da perícia forense digital quanto a eles.

Já quanto às características que trazem conectividade quanto ao sujeito do uso dos dados e metadados digitais, fazendo aqui menção direta à intangibilidade[48] e à sua valoração como evidência, e respectivamente como prova, deve-se deixar clara a ocasião de dificuldade quanto a quaisquer meios de garantia da integridade, devido sua natureza imaterial. É exatamente este pensamento ligado à valoração que se evidencia:

> [...]
>
> Sua proteção física e o cerceamento de contato de nada servem pois que seu valor não está em sua composição, mas em valores jurídicos que advém da ideologia nele representada (sua interpretação).
> [...]
>
> Todos esses dados têm um ponto em comum: não são materiais e nem são materializados por si. Os dados tratados pela informática nada mais são do que *bits* interpretados por dispositivos. Mas seu valor nas 3 (três) esferas da segurança informática são imensos. (SYDOW, 2022, p. 299-300).
> [...]

E o raciocínio continua neste sentido:

> [...]
>
> São, pois, obras originais, imateriais, intangíveis, existentes somente alocadas em um suporte material, que o grava por meios físicos, químicos, magnéticos ou outros. (SYDOW, 2022, p. 301).
> [...]

Tal pensamento é reafirmado quando se trata dos aspectos legais, e do modo como a legislação existente trata do tema, assim como também quanto às possíveis violações aos mesmos. Nota-se:

---

[46] **OLIVEIRA, Vinícius Machado. Identificação, coleta, aquisição e preservação da evidência. 2018.**
[47] **DANIELE, MARCELLO. La prova digitale nel processo penale. Rivista di Diritto Processuale, 2011. p. 292.**
[48] Conceito trazido por Sydow – **v. cf. SYDOW, 2022, p. 299-300.**

> [...]
>
> Ainda tratando da característica, é de se destacar o fato de que se tendo em vista serem os dados imateriais e, portanto, impalpáveis e de difícil percepção, os ataques a tais bens móveis serão comumente da mesma natureza, ou seja, virtuais, sendo a máquina do usuário-alvo sujeita a receber arquivos de dados com códigos maliciosos que darão ao dispositivo comandos prejudiciais a seu proprietário. Caso o ataque vise sistemas, ou haverá uma violação na máquina de origem ou haverá ingresso não autorizado no sistema e/ou nuvem com consequente obtenção de acesso aos dados. (SYDOW, 2022, p. 303).
>
> [...]

Já em se tratando da característica da conectividade[49], e ainda nas palavras de Sydow, tem-se que esta é demonstrada pela "capacidade tecnológica que um aparelho tem de se conectar com outros aparelhos e/ou com a rede"; e tendo a premissa de que não se detém meio de controle desta suposta conectividade, em razão da própria natureza dos dispositivos eletrônicos fabricados e consumidos atualmente pelos indivíduos, tem-se que a conectividade é uma característica fundamental para a compreensão do raciocínio acerca da instabilidade da integridade destas evidências digitais, bem como das provas. É o que se vê em:

> [...]
>
> A conectividade é uma importante característica. Quando um dispositivo é "autorizado" - no sentido técnico - a acessar a virtualidade através de um provedor de acesso, ele recebe um número denominado IP que passa a servir como um registro de acesso. A partir desse registro, denominado *log*, há uma autenticação do usuário, que passa a navegar ou utilizar-se de serviços. Toda relação de conectividade gera registros que têm guarda obrigatória segundo o Marco Civil da Internet, por determinados períodos de tempo. Tais períodos levam em consideração a necessidade de se registrar todos os percursos informáticos para resguardar as responsabilidades decorrentes das condutas informáticas, sejam criminais ou civis. (SYDOW, 2022, p. 288).
>
> [...]

Por fim, ainda se mantendo nas questões relativas às características dos dados digitais como evidência digital e prova digital, com intrínseca conexão quanto aos sujeitos/indivíduos que se valem destes dados e metadados digitais para cometimento de ilícitos, fala-se da anonimidade como um pilar fundamental para compreensão da complexidade para validação do uso de tais evidências/provas. Veja que tal aspecto é relevantíssimo para delinear muitas das problemáticas enfrentadas por todos os ramos do direito atualmente, em especial os ramos ligados ao Direito Penal e Direito Processual Penal. Tal debate será melhor enfrentado no tópico seguinte, tópico 4.

[49] Conceito trazido pelo Direito Digital – **v. cf. SYDOW, 2022, p. 287.**

3.1.1.1 As características dos dados digitais em nuvem - o *Cloudcomputing* e *Cloudstorage.*

Tendo sido abordadas as respectivas conceituações, há de serem esboçadas as características dos dados digitais em nuvem, no intuito de trazer o destaque e a relevância necessárias ao enfrentamento dos problemas fáticos, e até mesmo o debate acadêmico passar a ter mais conhecimento acerca da área e dos aspectos que envolvem os dados e metadados digitais contidos em nuvem.

Como raciocínio inicial, deve ser trazida a abordagem mais transparente possível sobre as características mais relevantes que permeiam os dados digitais em nuvem, bem como as peculiaridades presentes nestes em comparativo com os dados digitais contidos em *hardwares*[50] físicos, ainda mais tendo como premissa que todas as características destes também são inerentes àqueles contidos em nuvem, porém com algumas especificidades.

Um dos primeiros pontos a serem explanados diante da perspectiva dos dados digitais em nuvem são dotados de alta mobilidade[51], e neste ponto, vale ressaltar o pensamento de Sydow quanto à ausência de limitações da interatividade e conectividade dos dispositivos eletrônicos, é o que se mostra:

> [...]
>
> Somado à portabilidade dos aparatos, encontra-se p fato de que o desenvolvimento de tecnologias de satélite, ondas de rádio, a novel 5G e tecnologias populares e empresariais de acesso sem fio (*wifi*, conexão por balão, *starlink*, uso de rede elétrica, dentre tantas) permitiu que tais dispositivos, além de processarem informações de maneira móvel, também pudessem conectar-se uns aos outros e à virtualidade, sem limites ou restrições. (SYDOW, 2022, p. 284).
>
> [...]

Outra característica a ser exaltada é a de conectividade, inerente à "capacidade tecnológica que um aparelho tem de se conectar com outros aparelho e/ou com a rede"[52], que pode facilmente esclarecer o porquê de tantas inseguranças para com a disponibilização e o conteúdo dos dados e informações, contidos em meios digitais, os quais estejam inseridos em dispositivos eletrônicos munidos desta facilidade em interligarem-se com outros dispositivos, tendo em vista que nenhum indivíduo que preze gostaria de ter suas informações expostas, ou

[50] *Hardwares* são os dispositivos físicos e os sistemas eletrônicos que suportam as plataformas de processamento de dados digitais; Hassan correlaciona a importância do *hardware* quando do momento da criação de uma unidade de perícia forense digital – **v. cf. HASSAN, 2019, p. 87; p. 94/95**.
[51] Característica trazida pelo Direito Digital e Informático – **v. cf. SYDOW, 2022, p. 284**.
[52] Conceito trazida pelo Direito Digital e Informático – **SYDOW, 2022, p. 287.**

até mesmo fragilmente corrompidas diante de uma interligação não autorizada com outros dispositivos ou até mesmo a rede.

É justamente através destas características que vemos os diversos mecanismos e práticas antiforenses serem utilizadas, no sentido de trazer alguma violação à informação ou dado contido em ambiente digital ou virtualizado (é o caso dos vírus de computadores e smartphones), e realizando assim inclusive a conduta antijurídica punível. Neste sentido Sydow nos mostra:

> [...]
> Há, todavia, formas de se conectar a aparelhos informáticos explorando brechas de segurança, tomando conta da programação de um computador ou similar conectado e até mesmo enganando o usuário que, acreditando que a conexão (ou o pedido de conexão) é confiável, termina por autorizar em erro o pareamento dos itens estando sujeito à modificação não adequadamente autorizadas. (SYDOW, 2022, p. 287).
> [...]

Tais práticas serão demonstradas no tópico específico, mas nos servem de breve compreensão e reflexão das implicações geradas e das consequências aos diferentes ramos do Direito.

Seguindo com este pensamento, tem-se que, à partir das características já apresentadas, existe uma premissa sobre a impossibilidade de se determinar com exatidão qual a origem e o destino de determinada informação ou dado digital, aqui se falando em questões de territorialidade física, e é exatamente neste sentido que podemos fazer uma correlação direta para com a característica da mundialização[53].

A mundialização diz respeito à ausência de localidade que restrinja o acesso à determinada informação ou dado digital; pode-se acessar de qualquer lugar do globo. Neste sentido:

> [...]
> O conceito de mundialização, reconhecido expressamente no artigo 2º do Marco Civil da Internet (*A disciplina do uso da Internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: I – o reconhecimento da escala mundial da rede)* poderia ser substituído pelo de popularização da rede uma vez que anualmente tem-se notado aumento do número de pessoas denominadas conectadas. (SYDOW, 2022, p. 289).
> [...]

E neste mesmo sentido completa:

> [...]
> Ao relacionarmo-nos com um usuário da informática, com um internauta ou com pessoas jurídicas em rede, sempre resta uma sensação mista

[53] Característica trazida pelo Direito Digital e Informático – v. cf. **SYDOW, 2022, p. 288-289.**

> de proximidade somada à de incerteza quanto à localidade de onde partiu o acesso. (SYDOW, 2022, p. 289).
> [...]

Neste momento se faz altamente pertinente realizar um destaque à esta característica, principalmente no tocante à dados e metadados digitais contidos em nuvem, pois justamente por estarem sujeitas aos comandos típicos do *Cloudstorage* e do *Cloudcomputing*, são eles também que mais se utilizaram da característica de mundialização, devido sua intangibilidade e conexão direta com a rede, o que já traz também um entendimento de que podem ser acessados de qualquer região, em qualquer situação, de qualquer dispositivo eletrônico, desde que tal dispositivo esteja munido de conexão com a rede de internet.

Já fazendo um breve adendo, tendo também a interligação entre ambas, traz-se conjuntamente com a mundialização a característica da não territorialidade[54], que traz justamente esta noção conexa de impossibilidade de delinear com exatidão qual é a localidade específica onde se originou determinado comando, direcionado à determinado dado ou metadado digital, podendo tal comando abarcar situações delituosas que não respeitem linhas fronteiriças ou princípios norteadores do direito, como é o caso da jurisdição e da competência.

Tal discussão identicamente será deixada para o momento mais adequado, onde se realizará uma crítica assídua acerca da compatibilidade do uso de tais instrumentos, diante de suas características, frente aos institutos do Direito Penal e Direito Processual Penal.

Uma vez compreendidos alguns dos aspectos básicos que envolvem a transmissão de informações, dados e metadados digitais, bem como algumas das características inerentes aos dados digitais em nuvem, passa-se a uma compreensão mais aprofundada do procedimento que deverá acompanhar as investigações que deverão ser conduzidas sob determinada informação, dado ou metadado digital.

3.1.1.2 Etapas do procedimento forense digital

Realizadas as considerações iniciais quanto aos conceitos que envolvem os sistemas de transmissão das informações, dados e metadados digitais, é necessário compreender como funciona o procedimento de manuseio de determinada informação digital. Algumas das expressões a serem utilizadas nesta etapa de assimilação das informações relacionadas à esta procedimentalização forense digital, acabarão por trazer também noções introdutórias dos

[54] Característica trazida pelo Direito Digital e Informático – v. cf. **SYDOW, 2022, p. 308-309.**

aspectos jurídicos que envolvem o tema, bem como das problemáticas que irão se acarretar deste entrelaçamento que ocorrerá entre o cenário digital e o cenário jurídico.

Fazem parte do procedimento de investigação algumas etapas e protocolos para validação do uso daquela determinada informação, dado ou metadado digital que se quer ter como meio de prova para instruir um processo penal; parte deste procedimento é a submissão daquela determinada informação, dado ou metadado à uma formalização, aos olhos da norma vigente, de etapas concatenadas de autenticação da garantia de integridade daquela informação, dado ou metadado digital a que se quer fazer o uso[55].

Devem ser trazidas considerações acerca dos ramos da Tecnologia da Informação, voltados aos aspectos da perícia digital forense, no intuito de compreender os métodos adequados para realizar a devida procedimentalização da informação digital, e já compreendendo as dificuldades enfrentadas. Neste sentido, tem-se que os procedimentos forenses digitais são atualmente empenhados por uma estrutura investigativa própria, com aparato investigativo específico, o que claramente demanda uma capacitação profissional acima dos padrões normalmente impostos aos profissionais das demais áreas da Tecnologia da Informação; como se pode notar, todo o contexto investigativo de uma perícia forense digital é precedida de aspectos altamente técnicos.

Os técnicos e peritos forenses digitais são profissionais voltados para a análise e extração de determinados conteúdos e informações, contidas dentro de dados e metadados digitais, e não se limitando somente à isto, mas também passando para a respectiva instrumentalização desses dados, para ao fim da etapa investigativa, viabilizar o uso dessa informação ali contida no curso do processo criminal.

Para isto, o uso e observância às expressões normativas são de imperatividade absoluta, ainda mais levando em conta as etapas da procedimentalização do uso de determinada informação digital, e claro, levando em conta a norma vigente que regulará desta instrumentalização; algumas destas etapas trazem a necessidade de identificação, verificação, autenticação, isolamento, coleta, transporte, armazenamento e processamento daquela determinada informação digital[56] ao qual se quer fazer valer como meio de prova na instrução criminal.

Todas essas etapas são, já nos dias de hoje, um grande desafio aos operadores da máquina estatal investigativa, principalmente por parte dos peritos forenses digitais; vale trazer

[55] A cadeia de custódia já é trazida por Souza, com a importância da formalização de cada etapa da cadeia de custódia da prova, realizando a interligação do entendimento acerca da validade, licitude, bem como a finalidade probatória – **v. cf. SOUZA, 2020, p. 194-195.**

[56] As áreas da perícia forense digital trazem estas etapas – **v. cf. HASSAN, 2019, p. 42**. – pensamento interligado e corroborado pelo Direito Informático – **v. cf. SOUZA, 2020, p. 195-196.**

algumas ponderações feitas por alguns desses especialistas, principalmente para realizar o devido destaque no momento de analisar criticamente os métodos empregados, se comparados com os mecanismos existentes de melhor compatibilidade para realização dessas etapas.

Em primeiro momento, tem-se que deixar claro sobre a necessidade de criação de unidades investigativas capazes de realizar estas atividades[57], e aqui se fala de aparato estatal condizente com os mecanismos investigativos empregados pelos peritos forenses digitais; aqui se fala exatamente da criação de setores específicos e voltados para investigação exclusiva de dados digitais e o seu tratamento. Algumas das unidades da federação não detém tal aptidão, ou inexiste material humano capacitado, ou sequer detém recursos financeiros para viabilizar a construção e estruturação dos equipamentos necessários; eis aqui um primeiro desafio.

Existindo aparato capaz de realizar esta etapa inicial, passa-se à investigação forense digital, isto é, a obtenção, captação, extração e tratamento dos dados digitais que foram obtidos ao longo da investigação criminal convencional[58]. Nesta etapa se fala em adequação dos métodos empregados pelos peritos forenses digitais aos dados obtidos na investigação.

Os profissionais forenses trazem a etapa da identificação de IP do aparelho eletrônico investigado como sendo uma das primeiras etapas da devida análise pericial, isto pois qualquer erro cometido nesta etapa trará uma situação de alcance inexato de informações relativas à qual dispositivo eletrônico foi utilizado para o cometimento do ilícito, ou até mesmo obtenção de informações ligadas à aparelho eletrônico diverso, o qual não é objeto da investigação. É o que se extrai de Eleutério acerca dos IP's, veja:

> [...]
>
> O grande objetivo será descobrir qual computador estava utilizando o endereço IP naquele momento. Para isso, deve-se verificar no Registro.br para quem está registrado o endereço IP investigado. No caso de estar associado a um provedor de acesso (uma empresa de telefonia, por exemplo) será necessária uma nova etapa que consiste em obter com o provedor as informações sobre qual cliente utilizava aquele endereço IP na data e hora de interesse para a investigação.
> [...]
>
> Uma vez que o cliente foi obtido, é possível conseguir o endereço de sua residência (ou de uma empresa) a partir das informações de cadastro com o provedor. (ELEUTÉRIO, 2019, p. 109).
> [...]

[57] As áreas da perícia forense digital e Tecnologia da Informação trazem os requisitos de uma instalação forense digital – **v. cf. HASSAN, 2019, p. 84-85.**

[58] A perícia forense digital traz as etapas de obtenção da evidência digital – **v. cf. HASSAN, 2019, p. 120**. – bem como a análise destes dados contidas em dispositivo eletrônico – **v. cf. HASSAN, 2019, p. 145**. – pensamento que é corroborado pela apreensão, acondicionamento e tratamento destes dados – **v. cf. ELEUTÉRIO; MACHADO, 2019, p. 37/40.**

Porém, devem ser ressaltadas as peculiaridades acerca deste procedimento, conforme Sydow:

> [...]
>
> Desta maneira, a primária ideia de que o número de IP de uma máquina conectada à Internet levaria ao reconhecimento de um local físico tem perdido, não podendo ser tido como uma premissa absoluta há décadas. (SYDOW, 2022, p. 284).
> [...]

Clara a necessidade de cautela nesta etapa, pois, nos casos mau empenhados, corre-se o risco de acabar por trazer um desgaste do aparato investigativo, diante do esforço hercúleo para extração de dados digitais, os quais não terão proveito para a investigação, e podem inclusive ocasionar brechas, tanto no curso da própria investigação, de modo que o investigado se tornará mais cauteloso com seus dispositivos eletrônicos e com os dados contidos neles, quanto para o próprio processo que se desencadeará desta, de modo que as teses defensivas utilizadas no curso do processo irão explorar, cada vez mais friamente, essas brechas deixadas ao longo dos procedimentos investigativos[59].

Uma vez identificado o aparelho eletrônico que se faz uso para o cometimento do ilícito, tem-se ainda uma problemática quanto à pessoa que está na utilização daquele determinado aparelho eletrônico, no exato momento do cometimento do ilícito. Isto porque é facilmente dedutível a situação de que aparelhos eletrônicos são, em sua maioria, portáteis, e podem ser usados por quaisquer indivíduos com sua disponibilidade, o que claramente dificulta a definição de quem deveria ser o sujeito investigado.

Para sanar uma eventual presunção de tal situação, o que claramente seria possível de ser afastado por princípios do direito, tem-se existentes diversos mecanismos de autenticação do usuário do aparelho eletrônico, que é comumente chamado de autenticação de múltiplos fatores[60]. Estes mecanismos de autenticação basicamente se resumem em enviar algumas informações ao usuário do aparelho eletrônico, estas que somente poderiam ser confirmadas ou previamente sabidas por um usuário determinado, de modo que seja possível atingir uma resposta compatível com a informação enviada, dando assim uma "aprovação" naquela determinada etapa de autenticação, passando assim para a etapa seguinte, que trará novo procedimento autenticador, viabilizando assim a verificação adequada de que é ele quem está usando o referido dispositivo.

---

[59] Pensamento corroborado pela doutrina, quando discutida as nulidades processuais relacionadas ao tratamento inadequado de provas – **v. cf. NUCCI, 2022, p. 341-342.** – pensamento relacionado diretamente com a área de perícia forense digital – **v. cf. SOUZA, 2020, p. 48-49.**

[60] *Multiple steps verification procedures* - **v. cf. SYDOW, 2022, p. 119**.

São diversas as ferramentas utilizadas para realização destas etapas de autenticação, e todas essas ferramentas são concatenadas entre si, de modo que ao errar uma das etapas tem-se que iniciar todo o procedimento autenticador novamente. Este é o procedimento de autenticação de múltiplos fatores, e é um meio seguro de garantir a veracidade das informações utilizadas para confirmação de autenticidade, bem como para identificar o sujeito utilizador do aparelho eletrônico investigado. É o que ressalta Sydow:

> [...]
> Aliás, é por tal característica ser notória no meio informático e por ter grande importância nas relações informáticas que as identificações de autoria para procedimentos que geram responsabilidade (civil ou criminal) como *internet banking, e-mails*, uso de carteiras digitais, comunicadores instantâneos, uso de caixa eletrônico, operações de compras, dentre outras, usa métodos múltiplos de verificação: para verificar por mais de um meio e com maior grau de certeza tratar-se da pessoa autorizada aquela de quem veio a ordem. (SYDOW, 2022, p. 119).
> [...]

Tendo sido evidenciado qual será o sujeito investigado, bem como qual deverá ser o aparelho eletrônico objeto de perícia, passa-se à análise dos drives físicos e tangíveis contidos nestes, os quais internamente à eles estão os dados e informações digitais que se quer fazer uso. Para isto é necessário realizar a extração destes dados e informações; esta é a etapa de maior cautela, pois existem muitas minúcias para se atentar nesta etapa.

O devido procedimento pericial forense digital[61] traz ensinamentos ligados à necessidade de realização de uma cópia dos drives contidos nos dispositivos periciados, de modo a se manter íntegro o respectivo dispositivo, bem como de seus drives e dados nele contidos, para que se valha de uma atividade pericial adequada no material copiado, tendo assim um mecanismo de garantia da autenticidade dos procedimentos periciais empenhados no curso da análise forense. Ou seja, o material objeto de perícia deve ser copiado e mantido íntegro e resguardado nos devidos locais de armazenamento de evidências, enquanto que a cópia será analisada e possivelmente realizará a extração dos dados ali contidos, sem corrompê-las e sem realizar alterações.

Uma vez realizada a cópia de todos os drives relacionados do dispositivo eletrônico, far-se-á uma análise acerca dos dados e informações extraídas que tenham íntima conexão e com o objeto da investigação, devendo ser deixadas intactas quaisquer outras informações e dados que não estejam relacionados com os ilícitos investigados, sob pena de malferimento à

[61] O Direito Digital traz a importância da autenticidade como etapa preliminar do devido procedimento forense digital – **v.cf. TAMER; THAMAY, 2022, p. 40.** – bem como a etapa de obtenção adequada das provas digitais – **v.cf**. **op. Cit. p. 152.** – e a devida instrumentalização da cadeia de custódia digital – **v. cf. op. Cit. p. 167.**

direitos do investigado e violação à privacidade do mesmo. Aqui reside uma grande crítica, que será realizada em momento oportuno.

Esta etapa de extração[62] dos dados e informações digitais, contidas em dispositivo eletrônico periciado, é chamada de etapa de extração dos códigos hash[63], e é aqui onde residem os maiores problemas na utilização de dados digitais em nuvem, tendo em vista que a extração destes dados é muito mais delicada. Isto porque a utilização de códigos hash é feita de modo muito singular, a realização da extração do código hash é equivalente ao cálculo de uma conta do tamanho do peso do arquivo ou dado ou metadado ou informação digital ali contida.

Este é o pensamento exprimido pelo ponto de vista da perícia forense digital, veja:

> [...]
>
> Todas as suítes forenses oferecem recursos de hashing; no entanto, você pode usa uma ferramenta de terceiros ou apenas usar a ferramenta de hashing que existe como recurso interno do sistema operacional Windows.
>
> [...]
>
> No uso do PowerShell para cálculo do hash de um arquivo, por padrão o Windows emprega algoritmo SHA256; no entanto, você pode especificar a função hash criptográfica a ser usada adicionando o parâmetro ***-Algorithm*** após o caminh do arquivo segudo por um dos hashes criptográficos a seguir (SHA1, SHA256, SHA384, SHA512, MD5). (HASSAN, 2019, p. 63).
>
> [...]

A extração de códigos hash é a etapa em que se extrai determinada informação digital, de modo a gerar um código específico para aquela determinada informação, contendo caracteres específicos que remetem à ela, não sendo possível que o dispositivo eletrônico gere outro código similar para outra informação; somente é referente àquela.[64] É gerado um novo código toda vez que a informação foi acessada ou alterada, e este novo código não será igual ao anterior da informação originária.

Cada acesso e alteração, mesmo que meticulosamente feito, poderá ser comparada com a original através de um sistema de verificação entre os códigos hash fonte e os códigos hash cópia, e havendo qualquer mudança no código, um caractere que seja, tem-se a evidência de corrompimento da informação extraída, e consequentemente se torna uma brecha a ser explorada.

Além de trazer um referencial muito exato à informação que se está fazendo uso, é devido a esta singularidade que se torna possível verificar onde e como foi realizada a perícia nesta informação digital. De igual maneira se faz totalmente viável identificar e averiguar se a

---

[62] A etapa de extração do código hash, bem como seu cálculo é trazida pela Perícia Forense Digital – **v. cf. HASSAN, 2019, p. 62-63.**

[63] O conceito de função unidirecional *hash* e esclarecido sua conexão com o dado que se deseja extrair – **v. cf. ELEUTÉRIO; MACHADO. Desvendando a computação forense. 2019, p. 128-129.**

[64] A computação forense digital traz a definição de uma função hash, bem como as etapas de autenticação de modo figurativo – **v. cf. ELEUTÉRIO; MACHADO, 2019, p. 128-129.**

informação foi corrompida, modificada, alterada, cortada, editada ou até mesmo excluída por outro perito forense digital, através das técnicas antiforenses digitais.

Estes são os ensinamentos de Eleutério, veja:

> [...]
> O que torna esse tipo de função extremamente utilizada para a verificação de integridade de dados computacionais é o fato de que uma simples alteração na informação de entrada do algoritmo gerará uma sequência de bits (valor hash) totalmente diferente. Assim, se o conteúdo de um arquivo é submetido a uma função unidirecional e, em seguida, seu conteúdo é alterado em um único bit e submetido novamente à mesma função, duas sequências de bits completamente diferentes serão obtidas como resultado da função de autenticação, conforme ilustram as figuras 7.2 e 7.3. Dessa forma, utilizando este conceito, é possível se criar mecanismos seguros para a detecção de alteração em um conteúdo digital. (ELEUTÉRIO; MACHADO. 2019, p. 129).
> [...]

Em igual sentido se posiciona Hassan[65].

Nesta etapa tem-se a garantia de que determinada informação extraída é íntegra; que não houveram modificações para incriminar o investigado; que não houveram alterações para com a veracidade das informações ali contidas; que não houveram edições nem recortes para esconder parte daquela informação, no intuito de corroborar a atividade investigativa; que não houveram corrompimento de dados nem informações, viabilizando assim o uso integral desses no curso da investigação. Ou seja, nesta etapa se mantém a integridade do material extraído, bem como todas as condições de uso deste.

Devem ser extraídos os códigos hash, para serem utilizados de parâmetro frente aos dados originais, contidos no dispositivo eletrônico apreendido, o qual foi mantido íntegro na unidade investigativa de tratamento de evidências, para poder assim validar a compatibilidade de informações extraídas e periciadas, e demonstrar que a perícia forense digital agiu conforme todas as etapas adequadas de instrumentalização daquela informação. Esta é a devida adequação dos procedimentos forenses digitais aos dados e metadados digitais que são objetos da investigação, e é também o meio mais adequado para trazerem os indícios que se quer fazer prova, ou até mesmo a própria prova extraída do dado ou metadado digital.

3.2 Os aspectos técnico jurídicos e a óptica processual penal.

Feitas as apresentações iniciais sobre a temática da tecnologia da informação, dados e metadados digitais e do procedimento forense utilizado nas investigações, passa-se ao debate

[65] Esclarecimentos trazidos sobre a utilização deste conceito para segurança do dado digital – **v. cf. HASSAN, 2019, p. 62-63.**

acerca dos aspectos jurídicos que envolvem o tema, em especial os aspectos voltados aos ramos do Direito Digital, Direito Informático, Direito Penal e Direito Processual Penal.

Aqui serão inicialmente realizadas considerações acerca da norma penal e processual penal vigentes no sistema jurídico brasileiro, bem como das diferentes legislações esparsas que versam sobre o tema; será feita a análise das expressões utilizadas pelo texto normativo; os comandos que são emanados por esses textos normativos; a função que alí se esperava ser desempenhada pelo legislador que realizou a elaboração e promulgação daqueles textos normativos; será feita também uma análise das diferentes perspectivas que trazem maior enfoque ao tema e, por fim, serão trazidas as problematizações que envolvem o tema frente à estas diferentes perspectivas e modos de enxergar a situação.

3.2.1 Conceitos preliminares acerca do Direito Penal e Direito Processual Penal.

Primeiramente deve-se ressaltar que o procedimento e a etapa de produção de provas é ato essencial, tanto para o andamento correto do processo quanto para a devida aplicação de eventual entendimento jurídico do magistrado, que ali irá personificar a atuação do poder estatal frente às relações sociais e à norma que regula estas relações.

Deste modo, faz-se mister salientar que a função essencial da prova é conduzir um melhor entendimento sobre determinado fato, a fim de possibilitar ao julgador, bem como a todos os envolvidos no processo, que seja realizada a melhor atividade jurisdicional possível, exprimindo-se ali a situação mais próxima de uma "real verdade factual" e podendo assim então aplicar os conceitos contidos nas expressões da norma jurídica à realidade factual vivenciada por aqueles que estão envolvidos no processo.

Nesta linha de raciocínio, a prova é o meio ao qual se faz provar uma situação de fato, para que ao juiz fique claro e nítido qual a realidade de um fato, acontecimento ou episódio[66].

Para que sejam fornecidos ao juiz, elementos suficientes capazes de intentar em uma medida tão firme quanto é um processo de natureza penal, haverão de ser demonstrados todos os meios possíveis de cabimento e pertinência de determinada situação ao qual se quer provar, devendo assim fazer jus à medida imposta, justificada pela demonstração efetiva a qual se faz provar, pelos meios admitidos como tal, que determinada situação ocorreu[67].

---

[66] A doutrina que trata sobre o Direito Processual Penal traz a esta correlação da natureza da prova, bem como sua finalidade no curso da atividade jurisdicional – **v. cf. NUCCI, 2022, p. 27.**

[67] Entendimento deixado na norma – **v. cf. *caput,* do art. 155, do Código de Processo Penal – Decreto Lei nº 3.689/41**.

Deste modo, a prova pode se fazer através de diversos meios, e com diferentes finalidades, mas com um objetivo crucial, que é a capacidade de fazer determinada situação se tornar mais clara e segura a tomada de decisão e, por consequência, o exercício da atividade jurisdicional no uso do poder estatal e de suas atribuições.

Uma das considerações que deve ser realizada quanto ao procedimento de produção de provas é que, para a realização de uma instrução criminal, o conjunto probatório será revestido de características inerentes à finalidade da prova, ou seja, quanto ao seu sentido final, que é o de se fazer meio de prova. É o que afirma Nucci (2022, p. 29)[68] sobre os sentidos e classificações das provas (*sic*):

> [...]
>
> O termo *prova* possui, fundamentalmente, três sentidos: a) como *ato*: é o processo pelo qual se verifica a exatidão do fato alegado pela parte (ex.: fase de prova); b) como *meio*: trata-se do instrumento pelo qual se demonstra a verdade de algo (ex.: prova testemunhal); c) como *resultado*: é o produto extraído da análise dos instrumentos de prova oferecidos, demonstrando a verdade de um fato. (NUCCI. 2022, p. 29).
>
> [...]

Aqui se fazem essenciais tais distinções pois será discutido essencialmente a classificação e sentido da prova como um meio de trazer resultado ou de demonstrar-se a pertinência daquele fato com determinada circunstância que se quer realizar a prova.

Como já observado, as provas fazem um conjunto de procedimentos essenciais ao andamento e funcionamento do processo como um todo, mas também é necessário atentar para o meio de realização da produção de determinada prova, isto pois se aquela houver sido eivada de qualquer mácula, vício ou inobservância aos métodos, técnicas e protocolos exigidos, irá se acarretar em prejuízo ao exercício da atividade jurisdicional.[69]

Muitas vezes, poderão ocorrer situações de impunidade para com os agentes que cometeram aquele determinado fenômeno antijurídico, ou até mesmo em situações de violação à direitos e garantias individuais mínimas, o que configuraria uma inépcia estatal; isto porque, se declarada a ilicitude de determinada prova, não somente naquela irão incidir consequências jurídicas, mas sim em todo o decurso do processo e de seus atos realizados após a implementação daquela, devido ao raciocínio lógico concatenado que o processo jurídico traz em si. Desta mesma forma mostra-se:

> [...]

---

[68] O movimento doutrinário que lida com o Direito Processual Penal traz estas classificações acerca da prova – **v. cf. NUCCI, 2022, p. 29.**

[69] Este raciocínio se apresenta pela doutrina processual penal, de modo que a validade de tal prova está diretamente relacionada com a devida procedimentalização das etapas do processo penal, realizando correlação com o princípio da contaminação da prova ilícita – **v. cf. JUNIOR, 2023, 20ed, p. 1158.**

> De nada adiantaria preservar os direitos e garantias humanas fundamentais no nascedouro da produção da prova, permitindo-se, depois, a utilização de derivações flagrantemente inconsistentes, pois calcadas em alicerces podres. É o conhecido brocardo: "árvore envenenada não pode dar bons frutos". (NUCCI, 2022, p. 63).
> [...]

Como visto, faz-se mister dar uma ênfase maior na etapa da produção das provas para instruir um processo de natureza penal, em especial quando esta produção de provas se dá em contornos que envolvam uma informação, dado ou metadado digital, ainda mais levando em consideração sua natureza.

Nesta etapa deve-se trazer um escalonamento daqueles institutos, os quais trazem maior conectividade com o tema das informações, dados e metadados digitais, que é justamente a análise dos métodos, técnicas e procedimentos que são empregados pelos operadores da atividade jurisdicional, em especial voltados às informações e dados digitais, bem como às provas digitais contidas em nuvem.

Quanto aos métodos, técnicas e procedimentos utilizados pelos operadores da atividade jurisdicional, deve-se lembrar que o Código de Processo Penal[70] traz as disciplinas e os comandos normativos que irão regulamentar a utilização do aparato estatal para a validação da atividade jurisdicional, visando fazer a aplicação dos institutos previstos, fazendo uma adequação destes às demais legislações vigentes, de modo a trazer total capacidade do julgador em conduzir um raciocínio fundamentado, a fim de que seja empreendida a melhor solução possível ao caso factual apresentado à ele.

Trazendo uma breve alusão aos comandos normativos codificados, pode-se trazer o Título VII, do Livro I, do Código de Processo Penal[71], como exemplo do caminho que deve ser percorrido pelo julgador ao analisar cada aspecto da produção de provas, assim como também da utilização desta no meio processual para realização da atividade jurídica, passando desde a conceituação do que seria a prova para o processo penal, indo para uma capitulação de cada tipologia e espécie aplicada à este conceito, alcançando até mesmo o modo de execução de cada uma destas etapas relacionadas às espécies e tipos, e atingindo ao fim o procedimento como um todo e os regramentos à ele inerentes.

Em conjunto com os conceitos, tipos e espécies, modo de execução e procedimentalização de cada um destes institutos trazidos pela norma processual codificada, tem-se ainda a necessidade de adequação dos comandos normativos contidos nas demais

[70] Menção aos dispositivos normativos disciplinadores da devida procedimentalização – **v. cf. Capítulo II, do Código de Processo Penal – Decreto Lei nº 3.689, de 1941**.
[71] Op. Cit. – v. cf. **Código de Processo Penal – Decreto Lei nº 3.689, de 1941**.

legislações que versam sobre o tema das informações e dados digitais, como é o caso da Lei Geral de Proteção de Dados-LGPD[72], bem como a Lei do Marco Civil da Internet[73], que traz os regramentos, diretrizes e limitações do ente estatal, por consequência dos seus operadores, frente ao exercício deste poder, de modo a dar embasamento ao agente público estatal para agir corretamente, bem como também para frear suas ações em casos de eventuais temeridades.

Em alguns casos esta compatibilização entre a norma processual codificada e a norma extravagante contida em legislação específica ocorrerá sem trazer maiores complicações, fazendo assim com que o exercício do poder estatal através de seu agente, se mostre eficaz e atinja um maior nível de adequação à medida jurisdicional necessária ao caso factual.

Porém, em outros casos, pela mesma forma de pensar, a incompatibilidade de institutos jurídicos contidos na norma processual codificada, em detrimento de comandos normativos específicos contidos em legislações extravagantes, poderão trazer uma aplicação ineficiente e ineficaz para aquele determinado caso factual, gerando situações de impunidade, de insegurança jurídica, de contrariedade normativa e até mesmo jurisprudencial, e por fim gerando um cenário de enfraquecimento das instituições estatais que exercem a atividade jurisdicional.

Para adentrar na ideologia das provas digitais em nuvem, deve-se analisar o instituto das provas aos olhos do Processo Penal como um todo, para posteriormente prosseguir quanto à prova digital, e por fim adentrar na prova digital em nuvem.

Conforme pode-se extrair do pensamento doutrinário predominante no cenário jurídico acerca das provas, é possível se classificar as provas como sendo diretas ou indiretas, de acordo com a sua interligação com o que se deseja restar comprovado. É este o pensamento de Nucci:

> [...]
> São diretas as que se unem, sem qualquer intermediário, ao fato objetivado. São indiretas as que necessitam de interposto fatos, elemento ou situação para atingir o fato almejado. Em processo penal, admitem-se as provas diretas e as indiretas para qualquer fim: condenar ou absolver. (NUCCI, 2022, p. 42).
> [...]

Desta forma pode-se entender, que seja a prova utilizada como meio para obtenção do que se realmente almeja comprovar, ou seja ela utilizada como fim em si mesma para a comprovação factual, o resultado processual é um só, embasar o agente estatal na sua

[72] Dispositivo normativo que traz o tratamento de dados digitais pessoais, bem como o tratamento acerca do sigilo de dados, bem como os dados pessoais sensíveis dos indivíduos – **v. cf. Lei Geral de Proteção de Dados – Lei nº 13.709, de 2018.**
[73] Dispositivo normativo que regulamentou o uso e tratamento de dados digitais na Internet – **v. cf. Lei nº 12.965[73], de 2014.**

fundamentação para o exercício da atividade jurisdicional, em busca da verdade real, que é um dos princípios norteadores da norma, consequentemente da aplicação desta.

Esta foi a intenção do legislador ao realizar a promulgação da norma secundária contida no § 2º, do art. 157, do Código de Processo Penal[74], nota-se:

> [...]
> Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.
> [...]
> § 2º 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.
> [...]

De forma, contraposta à este entendimento, pode-se compreender que, em caso de eventual inobservância do comando normativo, ou de qualquer procedimento contido nele, geraria assim, uma nulidade objetiva do agente julgador frente ao objeto da comprovação factual que se buscava, ocasionando uma contaminação de todos os atos subsequentes àqueles considerados nulos; o que também é um dos princípios processuais norteadores da norma, através da teoria dos frutos da árvore envenenada. É o que está contido no comando normativo do *caput*, do art. 157, do Código de Processo Penal[75], veja-se:

> [...]
> Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.
> [...]

Tendo tal perspectiva em mente, pode-se passar à uma análise mais aprofundada acerca da prova digital e seu conceito, que seguindo o entendimento do comando secundário emanado no texto normativo processual codificado, em seu § 2º, do art. 157, pode ser encarada como toda e qualquer fonte comprobatória de algum objeto investigativo, desde que contido em meios digitais, sendo ela uma informação, um dado ou um metadado contido no em algum dispositivo ou aparelho eletrônico, ou até mesmo algum servidor externo, podendo assim ser acessado de diversos modos, inclusive através de plataformas de "*Cloud Computing*" ou "*Cloud Storage*", aqui já se tratando de provas digitais em nuvem.

3.2.2 Princípios relacionados ao Direito Penal e Direito Processual Penal.

[74] **BRASIL. Código de Processo Penal. 1941.**
[75] **Op. Cit.**

Para que seja feito um esboço dos efeitos e implicações trazidas pelo uso de dados e metadados digitais em nuvem no curso dos processos criminais, é necessária a abordagem preliminar de princípios norteadores do direito, em especial os princípios constitucionais penais[76], bem como os princípios do processo penal[77], e os entendimentos doutrinários acerca da compreensão basilar sobre os mesmos.

Passando assim então para uma perspectiva mais voltada às garantias individuais, tem-se que a posição doutrinária já é esclarecida quanto à necessidade de observância aos direitos fundamentais do processado em ação penal, nesta toada tem-se o princípio da legalidade[78], sendo talvez o medular entre eles, o qual nos traz a compreensão acerca da impossibilidade de atuação estatal extensiva à lei que o regulamente, deste modo então tem-se uma garantia primordial ao indivíduo, que dela se desentranham outros muitos, tendo inclusive proximidade direta entre eles, como é o caso da irretroatividade da lei penal[79], que por sua vez impede o agravamento da condenação penal nos casos de edição legislativa.

O mesmo pensamento aqui deve ser aplicado aos casos de crimes cometidos por meios digitais, seja se valendo deles para o cometimento do ato ilícito fim, seja como meio de alcance dos fins necessários ao cometimento do ilícito. De idêntica maneira, vai ser utilizado o mesmo raciocínio nos casos de edição normativa, para ampliar as prerrogativas estatais, nos casos de condenações que já ocorreram, mas que por alguma circunstância teriam tido melhor concretude probatória devido à alterabilidade normativa, no sentido de melhorar o aparato investigativo quanto ao tratamento de dados digitais que foram utilizados na condenação.

Assim como também não será possível realiza persecuções penais, contra indivíduos que anteriormente não haviam tipificação penal específica, quanto à seus delitos cometidos em meios digitais. Ou seja, os crimes cometidos em meios digitais, os quais ainda não foram regulamentados pelas entidades legiferantes, não poderiam ser investigados e punidos posteriormente à alteração legislativa positivada neste sentido para combatê-los, somente poderia abarcar situações futuras. Este é um ponto de altíssima importância para uma reflexão crítica posterior.

Voltando à análise principiológica, já analisando aspectos processuais penais, e em igual medida e importância, tem-se a presunção da inocência[80] como um pilar para a condução

---

[76] A doutrina traz os princípios constitucionais que se relacionam com o Direito Processual Penal – v. cf. **NUCCI. Manual de Direito Penal, 18ª ed. 2022, p. 20-21; p. 24; p. 27-28.**

[77] São trazidos os princípios que regem o Processo Penal, como o princípio da presunção de inocência – v. cf. **LIMA, 2020, 10ª ed. p. 47. –** o princípio do contraditório e da ampla defesa – v. cf. **op. Cit. p. 57-59**. – princípio da busca da verdade – v. cf. **op. Cit. p. 68-69**.

[78] **NUCCI, Guilherme de Souza. Manual de Direito Penal, 18ª ed. 2022, p. 42.**

[79] Também chamado por Nucci de "retroatividade da lei penal benéfica – **v. NUCCI, Manual de Direito Penal, 18ª ed. 2022, p. 20-21.**

[80] **NUCCI, Guilherme de Souza. Manual de Processo Penal, Volume Único. 4ed. 2023, p. 6.**

dos procedimentos investigativos, bem como para a própria instrução criminal, no sentido de jamais viabilizar atividade estatal punitiva de forma extensiva ao indivíduo sem antes ter coletado um amplo e vasto material probatório, e viabilizar identicamente o contraditório[81].

Já se valendo de contraditório, tem-se como elemento deste o devido processo legal[82], que é outro grande princípio elementar do processo criminal, devendo assim ambos andarem conjuntamente, de modo que qualquer indisposição à um causará consequentemente malferimento ao outro. O mesmo ocorre com a ampla defesa[83].

Não há o que se falar em devida instrumentalização processual, com intuito de condenação de um indivíduo réu em uma ação penal, que não tenha observados os devidos certames legais, bem como atuação jurisdicional compatível; caso contrário o que se terá é apenas uma atuação estatal punitiva e arbitrária, cheia de falhas e vícios, que além de não punir o agente, acaba por se igualar à ele na ínfima tentativa de alcançar uma condenação. Além de não fazer justiça, por mais que muitas vezes seja este o objetivo, também não traz proveito à atividade do ente estatal.

Toda esta explanação tem o fito de garantir um melhor esclarecimento sobre quais as maiores problemáticas que serão enfrentadas neste processo de compatibilização da norma, e de sua aplicação no cotidiano, para com os desafios enfrentados pelos operadores do Direito Penal, principalmente para viabilizar melhor visualização das respectivas críticas que devem ser feitas à cadeia de custódia digital e ao nosso sistema processual penal vigente

3.2.3 Implicações trazidas pelos dados digitais e dados digitais em nuvem ao Direito Penal e Direito Processual Penal.

Um primeiro olhar que se deve atrair para a discussão temática da validade do uso de provas digitais em nuvem no processo penal, é a observância das questões técnicas que envolvem o processo penal genericamente, voltadas à princípio para a produção de provas, que deverão respeitar os ditames de quaisquer outras provas comuns ao longo da instrução criminal.

Neste ponto vale destacar que a validade do uso destes dados e informações digitais, como meio de prova no curso de persecuções criminais, vai depender muito da adequação das normas de tratamento das provas convencionais para com os dados e informações digitais.

---

[81] **NUCCI, Guilherme de Souza. Manual de Processo Penal, Volume Único. 4ed. 2023, p. 9.**
[82] Tal debate é trazido juntamente com a conceituação do referido princípio pela doutrina – **v. cf. JUNIOR, 2023, p. 81-82.**
[83] Op. Cit.

A qualidade do dado e informação digital que está sendo selecionado para investigação; os meios e técnicas empregadas para garantir o melhor proveito daquela informação; o controle no tratamento e regulação do uso dos dados na etapa investigativa; o armazenamento adequado dos dados para checagem da integridade ao longo da instrução criminal; todas são etapas de alta imprescindibilidade, para garantir que seja dada a efetiva validade aos dados digitais que se fez uso no processo, caso contrário não terão o melhor proveito e consequentemente serão inválidas.

As provas digitais, diferentemente das provas comumente utilizadas nos processos penais, são caracterizadas pela volatilidade, mutabilidade e acesso facilitado[84], o que por si só acabam por ser geradores de desconfianças quanto aos procedimentos a serem utilizados para com estas provas, bem como também quanto à autenticidade, integridade[85] e eventual força que determinada prova digital irá exercer sobre aquela instrução criminal que está sendo realizada.

Neste ponto vale fazer um adendo, de modo a interligar todas as características anteriormente abordadas, para com os princípios do direito identicamente trazidos, no intuito de clarificar as diversas possibilidades que serão exploradas pelos indivíduos cometedores de ilícitos, tendo em vista que estes tentarão tirar o maior proveito dessas características, no intuito de burlar as normas contidas, achar-lhes contornos ou brechas, ou infringi-las sem que deixem rastros.

Feita esta consideração, tem-se que força probatória de determinado dado ou informação digital também estará condicionada à eficiência das técnicas empregadas, visando minorar-lhes as contaminações aos dados utilizados, evitar a alteração dos dados, de maneira a sempre mantê-los íntegros, e consequentemente trazer maiores certezas quanto à autenticidade da informação ali contida, fazendo se mostrar da maneira mais verossímil possível a devida conexão entre o indivíduo que se valeu do dado digital e o ilícito por ele cometido.

Tais condições objetivam assim uma melhor instrumentalização do procedimento investigativo e do processo como um todo, no intuito de não causar máculas à atividade jurisdicional exercida, e identicamente gerar mais segurança à todas as etapas da persecução penal, desde a fase inquisitorial até o cumprimento da decisão judicial de mérito.

Ainda em se tratando de dados digitais em nuvem, o risco é ainda maior para a realização de procedimento de produção de prova, haja vista que os dados digitais contidos em nuvem tem seu acesso disponibilizado à qualquer um que hoje tenha rede de internet[86] à sua

---

[84] Características trazidas pelos dados digitais – v. cf. **OLIVEIRA, Vinícius Machado. Identificação, coleta, aquisição e preservação da evidência. 2018. -** corroborado pela característica de manipulabilidade – **v. cf. SYDOW, 2022, p. 309.**

[85] A importância da autenticidade é trazida pelo Direito Digital – **v. cf. TAMER; THAMAY, 2022, p. 40.**

[86] Fazendo referência à característica da mundialização – **v. cf. SYDOW, 2022, p. 289.**

disposição, o que pode ser considerado como boa parte da população mundial, trazendo assim uma infinidade de possibilidades que acabam por gerar dúvidas e inseguranças à esta própria procedimentalização, às eventuais provas produzidas em si, e ao processo penal como um todo.

Mantendo-se a premissa das características altamente instáveis dos dados e metadados digitais, verifica-se que a alta disponibilidade dos memos trazem um grau extra de insegurança, quanto à alguns elementos essenciais à atuação criminal estatal repressiva, como é o caso dos elementos ligados à autoria, à dolo e culpa, à observância dos direitos e garantias individuais, e isto somente quanto ao indivíduo, já em relação aos delitos, temos a mesma ressalva com os elementos de materialidade, o nexo de causalidade, e de igual maneira tem-se as implicações ligadas à extraterritorialidade[87], à competência, à jurisdição.

Todas estas peculiaridades trazem à mingua os mecanismos empregados no curso de processos penais com uso de provas convencionais, se comparadas as provas digitais, isto porque uma real adequação normativa e jurisprudencial tem de ser realizada, no intuito de viabilizar a implementação e utilização da prova digital com maior serventia à persecução penal, podendo assim inclusive trazer benefícios ao andamento processual se adequadamente realizada a compatibilização dessas peculiaridades para com as práticas já existentes na legislação e nos diversos ramos de atuação pericial.

Ao mesmo passo que existe a real possibilidade de trazer maior eficácia e eficiência aos institutos do Direito, se empenhados adequadamente os esforços para enfrentamento das mudanças corriqueiras ligadas ao uso dos dados digitais, pode-se igualmente trazer diversas fragilidades e arbitrariedades, levando em conta a situação de defasagem dos instrumentos de regulação se comparados às inovações tecnológicas.

3.2.3.1 A evidência digital e prova digital no Processo Penal.

Em se tratando de material probatório para fins de persecução penal, interligado ao tratamento de dados e metadados digitais, no intuito de se atingir informações capazes de corroborar a medida repressiva estatal, tem-se a necessidade de delineação acerca do que se trata a evidência digital, o que pode ser classificado como indícios digitais, tanto ligados à autoria quanto aos de materialidade, do que seria a prova digital, e de como devem ser compreendidos cada um destes institutos, levando em conta seus respectivos conceitos em sua

[87] A extraterritorialidade é uma característica inerente aos dados digitais – **v. cf. SYDOW, 2022, p. 308.**

natureza primitiva, sem estarem relacionados com os meios digitais, para posteriormente trazer-lhes tal definição e compreensão.

A doutrina faz alusão à evidência e consolidação do *standard probatório*[88], como sendo um dos elementos essenciais para se dar início à fase inquisitorial dos procedimentos investigativos, e até mesmo um pressuposto para prosseguimento da ação penal em sua fase processual. Aqui já se fazendo alusão aos sistemas utilizados pelo estado brasileiro, no sentido de vigorar o sistema inquisitorial[89] na primeira etapa de investigações, e posteriormente adentrar na etapa relativa ao sistema acusatório fundamentado[90].

De idêntica maneira tem-se a ocasião interligada aos pressupostos mínimos para ambas estas fases, tanto em relação ao sistema inquisitorial, exercido em fase investigativa preliminar, quanto o sistema acusatório fundamentado, exercido na fase processual, são regidos por normas que determinam a necessidade de convalidação de seus respectivos procedimentos através de indícios[91] minimamente robustos e firmes, para dar-lhes ensejo ao uso das prerrogativas estatais necessárias à realização de atitudes de reprimenda.

Tal atividade não pode ser desmedida, neste sentido tem-se que a configuração dos indícios mínimos formam etapa de altíssimo grau de relevância em ambas as fases. Os indícios são, portanto, uma grande fonte de material comprobatório, ou auxiliarão na formação deste; sejam eles ligados à autoria, sejam eles ligados à materialidade, ambos detêm o poder de tornar o processo criminal uma ferramenta enviesada pelos olhos do operador que busca justiça, mas também detém o poder de credibilizar as atividades estatais empenhadas no intuito de fazer cumprimento à legislação concernente, sendo possível, ou não, inclusive que esta aplicação faça valer a justiça mais que a primeira posição enviesada. Tal crítica deve ser feita à posteriori.

Ainda se tratando de indícios, a primeira questão que deve ser correlacionada com os dados e metadados digitais é a situação de encontrar meios de se valer das ferramentas e institutos já disponíveis para alcance e formação dos elementos essenciais do que se tem por indícios, mesmo porque os indícios digitais[92] são de maior volatilidade[93], e trazem assim consigo uma maior dificuldade de se alcançar a soma de todos os elementos necessários para concretização dele.

---

[88] Entendimento demonstrado pela doutrina – **v. cf. LIMA, 2021, p. 585.**
[89] O sistema inquisitorial é a etapa utilizada no procedimento investigativo preliminar à ação penal, conforme demonstrado pelo entendimento doutrinário – **v. cf. JUNIOR, 2023, p. 10-11.**
[90] Também chamado de sistema *neoinquisitorial* – **v. cf. Op. Cit. p. 18.**
[91] Raciocínio demonstrado pela doutrina processual penal – **v. cf. LIMA, 2021, p. 576.**
[92] Correlacionando os conceitos de indícios também ao dado digital interligando com a norma, configurando assim o indício contido em meio digital – **v. cf. SOUZA, 2020, p. 333-334.**
[93] Característica trazida pela Tecnologia da Informação ao correlacionar com dados digitais – v. cf. **OLIVEIRA, Vinícius Machado. Identificação, coleta, aquisição e preservação da evidência. 2018**.

O mesmo ocorre com a evidência digital[94], mas com mais fragilidade, tendo em vista que a aplicação prática, da própria conceituação de evidência, se faz crer pela necessidade de um maior número de elementos, capazes de trazer convicção quanto ao cometimento do ato ilícito, ou pelo menos corroborar que ele ocorreu naquelas circunstâncias investigadas.

Isto ocorre muito quando se analisam pedaços ou partes de dados e informações digitais, mas sem ter acesso ao quadro completo destes, trazendo assim uma ocasião quase intuitiva por parte dos investigadores de qual deve ser o próximo passo a ser dado na busca do próximo pedaço ou parte; e não pode ser dessa maneira que ocorram as situações de formação de indícios e evidências. Não que seja este o caso de todas as investigações envolvendo dados e informações digitais, mas tem-se de ser levado em consideração esta possibilidade e tentar relativizá-la o máximo possível.

O quadro se assevera ainda mais quando se trata de prova em si, o conceito de prova[95] é algo já pacificado, no sentido de algo que se faz capaz de comprovar ou corroborar certas alegações ou suspeitas, e depende muito da natureza desta, podendo servir de fim em si ou de meio para alcance daquele; em qualquer um dos casos a prova é o instrumento que permeia toda a persecução penal, é o pilar central, por assim dizer.

Em se tratando de prova digital[96], esta tem o caráter idêntico da prova convencional, no sentido de trazer maior assertividade na tomada de decisão quanto ao que se está investigando, assim como também quanto à quem está se investigando, porém com a peculiaridade de se tratar de um material intangível[97], que por sua própria natureza tem a necessidade de tratamento mais adequado, bem como identicamente necessita de maior cuidado ao se valer dela como elemento fundante da decisão, isto pois qualquer mácula ocorrida no processamento dela afetará a decisão tomada anteriormente, bem como o restante do andamento processual.

Como conceito de evidência digital podemos dar destaque aos entendimentos de Hassan, veja:

> [...]
>
> A computação forense envolve a obtenção de evidências digitais, às vezes chamadas de informações armazenadas eletronicamente (ESI, electronically stored information), a partir da unidade de disco rígido de um computador, de um celular, de um tablet ou PDA, ou de outra mídia de armazenamento (como CDs/DVDs e pendrives), entre outros locais, de

[94] Traz a conceituação, bem como as classificações de evidência digital – **v. cf. HASSAN, 2019, p. 35.**
[95] Conceito e classificação trazidos pela doutrina do Direito Penal – **v. cf. NUCCI. Provas no Processo Penal. 2022, p. 29.**
[96] Souza realiza uma conexão entre o conceito de prova para com os elementos digitais, com o fito de criar a figura da prova digital e sua conceituação de acordo com a norma – **v. cf. SOUZA, 2020, p. 35-37. –** conceito corroborado e trazido pelo Direito Digital – **v. cf. TAMER; THAMAY, 2022, p. 32.**
[97] Característica trazida pela doutrina do Direito Digital e Informático, quanto à intangibilidade – **v. cf. SYDOW, 2022, p. 299.**

> maneira sistemática; essas ESI serão usadas na corte durante julgamentos. (HASSAN, 2019, p. 35).
> [...]

Já no tocante à prova digital, temos que o posicionamento doutrinário se mostra ainda em consolidação, mas já traz compatibilidade com os conceitos preliminares de prova, é o que se mostra nos estudos de Thamay e Tamer[98], nota-se:

> [...]
> A dita prova digital continua, na essência, sendo prova, como dito, o instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato, e em caso positivo, delimitar todas as suas características e circunstâncias, respondendo não só a pergunta se o gato ocorreu ou não, mas como ocorreu e quais sujeitos estão a ele atrelados, ativa ou passivamente. (THAMAY; TAMER. 2022, p. 32).
> [...]

O mesmo se mostra em quanto as ressalvas no tocante ao tratamento mais adequado anteriormente citado, fica claro em:

> [...]
> A utilidade da prova digital passa necessariamente pela observância de três fatores principais: (i) autenticidade; (ii) integridade; e (iii) preservação de cadeia de custódia. (THAMAY; TAMER. 2022, p. 40).
> [...]

É neste sentido que se tem a similar compreensão acerca dos indícios, estando eles ligados à autoria ou à materialidade, ambos têm a necessidade de trazer a conexão entre certo fato e determinada prova deste, nas palavras de Renato Brasileiro de Lima, é o meio pelo qual *partindo-se de um fato base comprovado, chega-se, por meio de um raciocínio dedutivo, a um fato consequência que se quer provar*.[99]O mesmo raciocínio se aplica ao indício digital.

Enfrentadas as compreensões preliminares acerca das consequências e implicações trazidas, bem como as respectivas conceituações do que se trata a evidência e a prova digital, para prestabilidade e utilização em persecuções criminais, passa-se ao desenvolvimento do entendimento acerca da cadeia de custódia, de modo que faz-se imprescindível este às críticas empenhadas, isto pois a chamada cadeia de custódia digital prescinde destas noções anteriormente esboçadas, até porque reside aqui o ponto focal acerca das maiores mudanças e inovações tecnológicas enfrentadas pelos operadores do Direito, bem como os operadores da Tecnologia Digital em suas respectivas atuações forenses.

Fica clara a interdisciplinaridade entre as áreas da Tecnologia da Informação para com os ramos de atuação do Direito, em especial no tocante aos procedimentos investigativos, às

[98] **TAMER; THAMAY, 2022, p. 32.**
[99] **LIMA. Manual de Processo Penal: vol. único, 2021, p. 576.**

perícias, toda a matéria probatória, a composição do dolo e da culpa, a materialização da medida judicial compatível ao caso concreto que fez o uso de dados e metadados digitais, tudo isto no intuito de trazer a efetivação de melhores medidas que satisfação a norma processual penal vigente, conjuntamente com as garantias constitucionais, para com este cenário descrito.

3.2.3.2 A Cadeia de Custódia Digital.

Para uma compreensão acerca dos instrumentos que permeiam os ambientes de operacionalização virtual das atividades e relações sociais, e sua intrínseca relação com o devido processo legal e as garantias individuais, bem como quanto às discussões pertinentes ao tema, pode-se destacar as práticas realizadas pelos agentes antijurídicos ao empregar técnicas especializadas capazes de dificultar, e em algumas ocasiões até mesmo inviabilizar, as atividades dos agentes investigativos estatais que irão proceder no combate à essas atividades.

No referente aos aspectos técnico-científicos inerentes à Tecnologia da Informação, deve-se dar enfoque aos fenômenos dos VPN's[100], que são meios de ocultação do IP de determinado dispositivo eletrônico, com finalidade de utilizar de uma rede corporativa diversa da que é pertencente ao IP original do dispositivo, gerando assim uma conexão privada entre o dispositivo eletrônico e o endereço virtual que se busca conexão, é o que se afirma em:

> [...]
>
> Um serviço de VPN permite que você crie uma conexão privada, criptografada entre seu computador e o site que você visitou. Você pode proteger seu computador de software malicioso, proteger uma rede de Wi-Fi, mudar seu endereço IP ou trabalhar remotamente em uma rede corporativa. (ZAREMBA, 2015).
>
> [...]

Neste ponto, é necessária fazer a interligação entre o campo da Tecnologia da Informação e o campo do Direito, em especial os ramos do Direito Processual Penal, devendo-se dar destaque especial à cadeia de custódia, pois como demonstrado, alguma das técnicas empregadas pelos indivíduos cometedores dos fenômenos antijurídicos, são de ocultação para com as suas assinaturas digitais, que eventualmente iriam possibilitar aos agentes estatais investigativos.

Já se voltando aos aspectos técnico-jurídicos da discussão temática, como anteriormente dito, deve-se dar enfoque à cadeia de custódia contida no curso dos processos penais, e já pensando em aspectos processuais é imprescindível verificar os dispositivos legais

[100] VPN são também chamados de *virtual private network*, são redes privadas de conexão criptográfica – entendimento trazido pela Tecnologia da Informação – **v. cf. PROKISCH, 2023, p. 39.**

que envolvem esta ótica, frisando os arts. 158-A, 158-B, 158-C, 158-D, 158-E e 158-F, do Código de Processo Penal[101], que irão disciplinar a atuação dos agentes estatais investigativos na instrumentalização da devida atuação, de modo a ser condizente com as técnicas e fenômenos antijurídicos realizados pelos indivíduos objeto destas diligências.

Para que um entendimento maior acerca dos institutos normativos supracitados seja possível, há de ser imperativo o destaque à inafastabilidade da observância da norma, ainda que se tratem de procedimentos específicos da atividade jurisdicional, em especial os procedimentos voltados ao processo penal, que devem ter uma aplicabilidade normativa imprescindível sob pena de nulidade, é o que se extrai:

> [...]
> As nulidades são vícios ou falhas processuais, que podem macular a construção de provas, a constituição correta do rito procedimental ou de qualquer outro ato ou peça inerente ao feito.
> Nulidades não constituem institutos jurídicos autônomos, com *vida própria*, dispostos a estudo aprofundado. São meros defeitos dos atos e fatos processuais, diante do desrespeito a fórmulas previamente estabelecidas em lei. (NUCCI, 2022, p. 341).
> [...]

Em se tratando de institutos processuais específicos, como é o caso da cadeia de custódia, ainda que estes institutos tratem de forma abrangente à quaisquer meios de diligência, mesmo não frisando e mesmo não se mantendo adstrito à cadeia de custódia dos dados digitais, ainda sim revelam-se imperiosos os esforços para manutenção e observância às condições legais impostas de modo geral, de modo a possibilitar a aplicabilidade dos institutos gerais aos dados e informações digitais; em conformidade com este entendimento pode-se notar:

> [...]
> Malgrado o código de processo penal não verse especificamente sobre o vestígio digital, as regras expostas nos artigos 158-A a 158-E são também observáveis quanto ao dado cibernético e a norma ABNT 27037:2013, anterior inclusive ao pacote "anticrime", estabelece as regras para a preservação da cadeia de custódia digital.
> Com efeito, a norma ABNT 27037 descreve e define as "Diretrizes para identificação, coleta, aquisição e preservação de evidência digital", apresentando, resumidamente, as seguintes etapas a serem observadas: Identificação, Coleta, Aquisição e Preservação (OLIVEIRA, 2019) *sic*. (COLAVOLPE, 2022, p. 178).
> [...]

De igual forma pode-se destacar a perspectiva de necessidade de adaptação dos operadores destes institutos normativos, de modo a possibilitar uma aplicabilidade eficiente desses instrumentos, evitando assim uma atividade jurisdicional deficitária e evitando também

[101] Menção direta aos dispositivos normativos contidos no Capítulo II, do Código de Processo Penal - Decreto Lei nº 3.689, de 1941 – **v. cf. BRASIL, 24 out. 1941.**

divergências entre a aplicação destes instrumentos por um agente estatal em detrimento de outro agente que irá aplicar a mesma norma, porém com sentido diverso, gerando assim "brechas normativas" que se valeriam os indivíduos cometedores de fenômenos antijurídicos, por exemplo, brechas estas que se dariam em determinada localidade e não se apresentariam em outras, ou até mesmo brechas que se valeriam em determinado tema ou enfoque e que poderiam ser descartadas em outra temática ou enfoque.

Trazendo a questão da observância aos comandos normativos novamente ao debate, fica implícita a situação de acarretamento e fornecimento de melhores condições aos agentes aplicadores da norma, para que possibilite a realização de melhores práticas por parte desses, a fim de incentivar a abstenção das práticas antijurídicas por parte daqueles que se valeriam das brechas impostas pela eventual ineficiência dos agentes investigativos estatais.

Já se voltando aos procedimentos normativos em face dos dados e informações digitais, faz-se imperioso lembrar dos comandos contidos no texto legislativo codificado processual, em especial os comandos contidos no Capítulo II, do Título VII, do Código de Processo Penal, é o que se mostra também no entendimento doutrinário por Sydow:

> [...]
> Em seguida, corroborando o Princípio da Manipulabilidade do Elemento Informático, aponta que a admissibilidade do elemento informático na investigação e no processo exigirá a disponibilidade dos metadados e a descrição dos procedimentos de custódia e tratamento suficientes para a verificação da sua autenticidade e integridade.
> [...]
> Aponta expressamente os meios de obtenção dos elementos como sendo (I) a busca e apreensão de dispositivos eletrônicos, sistemas informáticos, ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo; (II) a coleta remota, oculta ou não, de dados em repouso (estáticos) acessados à distância; (III) a interceptação telemática de dados de transmissão (dinâmicos); (IV) a coleta por acesso forçado de sistema informático ou de redes de dados; e (V) o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial. Isto esclarece à sociedade os principais meios e reforça a legalidade da Investigação Defensiva. (SYDOW, 2022, p. 728)
> [...]

Fica claro que é de preocupação de toda a comunidade jurídica, e não somente ela, a devida adaptação da atuação estatal frente à estas peculiaridades trazidas pelos campos de atuação da Tecnologia da Informação, em especial os dados e informações digitais, que acabam por trazer um cenário de incerteza e desconfiança para com as próximas etapas de evolução destes meios tecnológicos, e que se encontram em enorme disparate para com a evolução das normas jurídicas, e tal preocupação é decorrente da deficiência dos órgãos legiferantes em atribuir as devidas conceituações, as devidas medidas, e o devido esmiuçamento ao abordar as

técnicas que deverão ser empregadas para com as peculiaridades apresentadas pela esfera técnico-científica dos dados e informações digitais que compõe o ramo do Direito Informático.

Conforme o entendimento de boa parte dos autores doutrinários que já se inseriram nas discussões temáticas acerca do Direito Informático, a questão principal entorno das peculiaridades trazidas pelos dados e informações digitais é a situação de manter aquele determinado dado e informação digital hígido e sem alterações até que sobrevenha uma análise técnico-jurídica acerca da validade daquele dado como parte do processo, e claro, se a devida procedimentalização ocorreu ao se realizar a extração, coleta, manutenção e processamento daquele determinado dado ou informação digital.

Nesta mesma linha de raciocínio se mostra:

> [...]
>
> E, para que tal verificação seja fidedigna, é indispensável a preservação ou conservação (custódia) de todos os elos da cadeia probatória, de modo que seja possível percorrer todo o caminho dos vestígios, desde a sua coleta até a análise pelos peritos, e confirmar a origem lícita, bem como que não houve substituição, contaminação ou adulteração daqueles elementos de convicção colhidos no curso da investigação e do processo penal.
>
> Essa preservação dos vestígios passou a contar com minuciosa regulação, inscrita nos arts. 158-A, 158-B, 158-C, 158-D, 158-E e 158-F, incluídos no Código de Processo Penal através da recente Lei 13.964/2019. O regramento prevê detalhadamente os protocolos a serem observados desde a fase regulada pelo art. 6º do Código, passando pelo "reconhecimento", "isolamento", "fixação", "coleta", "acondicionamento", "transporte", "recebimento", "processamento", "armazenamento"e "descarte" dos vestígios, abrangendo, assim, todas as fases do da *(sic)* caminhada daqueles e prevendo meios adequados para que sejam conservados de forma segura. (SOUZA, 2020, p. 195-197).
>
> [...]

Conforme se extrai do entendimento demonstrado, as diretrizes acerca dos comandos normativos, bem como dos procedimentos utilizados para uma eficiência na atividade jurisdicional, estão diretamente relacionados com a devida adequação da atividade dos agentes investigativos para com as condutas e etapas de procedimentalização, frente às peculiaridades apresentada pelos fenômenos antijurídicos, aos quais se valem das eventuais brechas ocasionadas pela inobservância dos comandos normativos, pelos mesmos agentes investigativos ao longo do curso do processo, ocasionando assim uma eventual porta de entrada, para que àqueles se valham dos dados e informações digitais através de práticas criminosas, ou até em último caso, gerar uma nulidade processual a ser utilizada pelo investigado, para se valer de impunidade em situações que em outras circunstâncias poderiam ser prevenidas e então devidamente comprovadas.

No raciocínio apresentado, e no intuito de conciliar os entendimentos acerca de um caminho adequado e compatível para o devido tratamento de dados e metadados digitais, diante dos dispositivos normativos existentes, se apresenta lógica a compreensão acerca do resguardo dos dados digitais originários, bem como dos dispositivos eletrônicos e aparelhos apreendidos, os quais são objetos da investigação.

Tal resguardo do material originário, bem como do *hardware* físico apreendido, pode ser realizado de modo a criar uma simples cópia do material, em sua íntegra, de modo a gerar códigos de extração *hash*[102] pra ambos os dados colhidos, tanto o original quanto o copiado, de modo que as investigações, alterações de dados, emprego de técnicas criptográficas reversas, bem como demais atividades dos agentes periciais acabem por resultar em uma comprovada metodologia no tratamento dos dados objetos da perícia. Este raciocínio será melhor explorado no capítulo crítico, bem como trazer o comparativo dos códigos de extração originários face à face com os examinados na perícia.

Desta forma, demonstra-se assim a autenticidade da informação ali contida, bem como sua originalidade de informação e imutabilidade daquilo que se tornará objeto de prova, ou prova como fim, no curso da investigação criminal. Isto se da pois cada alteração no código extraído que foi objeto de alteração ou mudança não autorizada ou não controlada pelo devido procedimento, não será comparável com a informação original, ou pelo menos acusará onde foi feita a alteração e que ela não é igual àquela anterior utilizada na perícia, não servindo assim como meio de obtenção para prova ou como prova em si, devido a violação da cadeia de custódia digital utilizada naquele determinado dado ou metadado digital; tal análise será melhor esclarecida na crítica do capítulo próprio, e a coisa se complica mais no cenário do dado digital contido em nuvem.

3.3 Interdisciplinaridade e as implicações nos devidos procedimentos investigatórios e processos penais em curso.

Tendo brevemente abordado parte dos conceitos preliminares, bem como suas características, tanto voltadas aos aspectos tecnológicos dos dados digitais quanto aos aspectos jurídicos e processuais, visa-se realizar uma interligação entre tais perspectivas, demonstrando de forma concatenada sua conexão.

[102] Os códigos de extração hash tem seu valor computacional diferido para cada informação digital contida, de modo que cada código extraído é diferençável dos outros dados digitais analisados – entendimento trazido pela Tecnologia da Informação, com principal enfoque pela perícia forense digital – **v. cf. HASSAN, 2019, p. 128-129**. – pensamento já compreendido pelo movimento doutrinário do Direito Penal – **v. cf. BAQUEIRO; CAVALOPE, 2022, p.180.**

Demonstrados alguns poucos aspectos da era digital e dos sistemas de dados digitais em nuvem, pode-se compreender como estes fenômenos contidos nos campos da tecnologia da informação acabam por suceder em inevitáveis consequências quanto às relações sociais, o que por conseguinte trazem também às atividades ligadas ao ordenamento jurídico como um todo, que regulam essas relações sociais, em principal as atividades jurisdicionais direcionadas à regulação dos crimes, ou chamados cibercrimes.

O devido procedimento investigativo deve seguir os parâmetros necessários para a identificação correta do indivíduo que estava se valendo daquele determinado servidor de acesso externo, através de uma plataforma ou serviço de "*Cloud Computing*", para realizar a prática de atividades antijurídicas, podendo assim o ente estatal se valer da ferramenta adequada para coibir a continuidade destas atividades, observando sempre os princípios relacionados ao exercício da atividade jurisdicional, tanto na esfera penal quanto na esfera processual.

É aqui onde se mostram imprescindíveis a observância aos preceitos jurisdicionais estipulados pela norma, a necessidade de profissionais aptos e capacitados para realizar as práticas de atividades forenses digitais, em especial voltadas às atuações investigativas, bem como também a delimitação concreta do que será objeto da investigação forense digital.

O primeiro passo para preenchimento destas etapas é a identificação adequada do aparelho ou dispositivo que está sendo utilizado para a prática de determinada atividade antijurídica, em segundo deve ser realizada a identificação do indivíduo que estava se valendo daquele determinado dispositivo, naquele determinado momento, realizando aquela determinada atividade.

Posteriormente, deve ser verificada se aquela determinada prática antijurídica tem regulamentação específica do modo de realização dos procedimentos que envolvem a atividade investigativa, em caso positivo deverá observar a regulamentação específica, em caso negativo deverá observar a regulamentação processual e procedimental contida nos instrumentos normativos codificados.

Por fim, deve-se observar se a realização dos procedimentos investigativos está sendo utilizada como um fim em si mesmo, que seria a busca da informação ou dado digital como o material investigativo em si, ou se é apenas meio para obtenção de um fim, que seria a busca do material investigativo factual ao qual apenas se usou de determinada informação ou dado digital para obter alcance deste.

A ratio contida no caminho a ser percorrido pela autoridade investigativa forense digital é a situação inerente às características dos dados digitais como um todo, em especial os contidos em nuvem. É o que se afirma (*sic*):

> [...]
> Compartilhamento de recursos é característica importante pois representa que o provedor do serviço atende simultaneamente múltiplos consumidores, alocando seus recursos de modo dinâmico, conforme a necessidade da demanda. Há, assim, uma sensação de independência de localização posto que o consumidor não possui poder de decisão, controle ou conhecimento sobre o exato local dos recursos do provedor – podendo conhecer genericamente o local ou *datacenter* onde estão os dispositivos. Aqui, a característica de PLURALIDADE a ser apresentada adiante. (SYDOW, 2022, p. 76).
> [...]

De idêntica forma mostra-se em (*sic*):

> [...]
> Por isso é necessário sempre lembrar que o dispositivo de um usuário pode ser usado como um zumbi (instrumento ou ferramental), seu computador pode ser aproveitado como meio (desvio de função de instrumento) ou, ainda, seu acesso pode ser sito usurpado e os logs de acesso indicam e presumem erroneamente a autoria.
> Portanto, não é simples a tarefa de acusação em delitos informáticos, porque além da presunção de inocência constitucional, a informática impõe um especial cuidado pela grande gama de alternativas de cometimento da ação juridicamente reprovável. Há, por isso, uma segunda presunção de inocência denominada técnica. (SYDOW, 2022, p. 328).
> [...]

Nota-se já adentrar na esfera jurídica trazida pela influência da era digital no contexto factual das relações sociais, deste modo deve-se dar a ênfase adequada à elas no ponto de vista jurídico que regulamentará essas relações e essa atividade antiforense digital, realizando suas respectivas críticas e análises aprofundadas, devendo assim ser abordada em tópico específico subsequente, tendo como premissa as demais conceituações e informações trazidas neste capítulo.

4. Análise crítica

É neste contexto, de problematização do uso e validação das provas digitais em nuvem no processo penal, que se insere a discussão temática, sendo identicamente realizada uma análise legislativa sob as regulamentações vigentes, assim como também das que estão por surgir ou em fase de elaboração de projeto, com o fito de garantir uma abordagem temática completa, levando em conta as diferentes possibilidades apresentadas pelo contexto normativo vigente, bem como do modo de enfrentamento pela jurisprudência das situações fáticas, as quais são cada vez mais frequentes e problemáticas para o ordenamento jurídico atual; isto levando em conta que o atual Código de Processo Penal é uma codificação normativa da década

de 1940, e que, mesmo tendo ocorrido algumas alterações legislativas, está longe de abarcar adequadamente os procedimentos necessários para empenho de uma boa atividade jurisdicional.

Algumas das considerações de maior relevância quanto ao tema discutido podem ser direcionadas às questões de garantias mínimas em que o indivíduo pode se valer de meio de proteção para com a atividade estatal abusiva, das limitações que o exercício do poder estatal deve obedecer a fim de evitar o malferimento à garantias e direitos individuais; assim como também, algumas destas considerações estarão voltadas às necessidades de implementações de técnicas eficientes e eficazes, para o combate e repressão de atividades antijurídicas por parte da sociedade, mas que da mesma forma possam respeitar as balizas mínimas que devem ser asseguradas aos investigados.

Não obstante à ótica das garantias individuais, serão identicamente explicitadas as situações fáticas que exigem maior cuidado pelo ponto de vista estatal, desta forma será discorrido sobre as técnicas empregadas pelo Estado para realizar o exercício do seus poderes, quais dessas condizem melhor com as realidades cotidianas da sociedade, quais dessas tem maior compatibilidade com a realidade do cenário da evolução tecnológica e cibernética, e como as implicações destas técnicas acabam por ocasionar afetação nas relações sociais cotidianas e no controle destas relações.

Estes são apenas alguns dos diversos prismas a que se pode ter acesso, somente em uma análise preliminar das realidades sociais que estão entrelaçadas com o Direito, e aqui se faz somente uma abordagem nos campos do Direito Digital e Direito Informático e sua relação com o Direito Penal e Direito Processual Penal, sem abordar aspectos civis, os quais com toda certeza tem implicações bem mais diversas e identicamente severas. É o que se extrai:

> [...]
>
> Na perspectiva da segurança pública, nós perguntamos, por exemplo, quando temos a discussão relacionada ao direito à privacidade sob a perspectiva de garantia da segurança pública. Nós temos a possibilidade de que o Estado utilize justificativas cíveis e penais? Por exemplo, se nós tivermos uma situação de catástrofe ou de calamidade pública, como recentemente, o Estado pode acessar os dados do cidadão para garantir a segurança de determinada região?
>
> [...]
>
> O reconhecimento facial disseminado, tal como está ocorrendo, é um cenário de hipervigilância, sob a perspectiva de garantir a segurança pública. Como o reconhecimento facial em aeroportos, em transportes públicos e em eventos. Isso torna a segurança um pouco mais eficaz ou eventualmente pode fazer com que, a pretexto de segurança pública, se tenha um controle estatal privado de dados individuais? E como vão manusear essas informações? Como vai ser feita a utilização e o descarte disso?. (MUDROVITSCH, 2022, p. 165).

[...]

Então, demonstrar-se-ão as diferentes perspectivas, tanto do ponto de vista "legalista" da problemática quanto do ponto de vista "garantista", acerca dessas afetações no universo jurídico da sociedade como um todo, levando ainda em consideração a base da relação social para com o ente estatal e os aspectos científicos que englobam todo o contexto evolutivo destas relações sociais com tal ente, vislumbrando claro, sob um enfoque às áreas do Direito Penal e Direito Processual Penal.

4.1 Os métodos e mecanismos atualmente empregados quanto ao uso da prova digital no processo criminal.

Após toda a concatenação lógica acerca dos raciocínios apresentados sobre as características e conceitos dos dados e metadados digitais, sobre o procedimento forense digital, sobre os princípios materiais e processuais envolvidos no tema, bem como da respectiva interdisciplinaridade entre as áreas que envolvem o Direito Digital, o Direito Informático e o Direito Penal e Direito Processual Penal, aprofunda-se a análise dos meios utilizados recentemente pela atividade estatal, pela perspectiva técnico-científica, e pela análise da instrumentalização problematizada destes setores.

Além do cenário de problematização dos setores envolvidos no tratamento dos dados digitais e suas implicações com a utilização pelos agentes estatais, traz-se ainda outras questões pertinentes ao desenvolvimento tecnológico e como podem ser abordados diferentes técnicas e caminhos para sua respectiva adequação ao cenário fático do uso dos dados digitais no curso dos processos criminais.

As diferentes perspectivas passam desde análises dos dispositivos existentes e debate sobre adaptação viável destes, até mesmo a análise de dispositivos normativos e legislações estrangeiras para melhor compreensão acerca do tema; por fim levantam-se alguns questionamentos correlatos no sentido da viabilização dos debates futuros a serem abordados nas respectivas áreas.

4.1.1 Mecanismos existentes, meios de utilização, procedimentos empregados, capacidades técnicas dos peritos e investigadores digitais. (seja ela digital em mídia física seja ela digital em nuvem).

Nesta altura do debate já se têm compreendidas as questões problemáticas trazidas pelo tema, de modo que resta uma análise de quais procedimentos vêm sendo empregados pelos agentes investigativos periciais atualmente, bem como os demais órgãos do Poder Executivo e do Poder Judiciário, assim como também qual o entendimento jurisprudencial vem sido praticado, pelos Tribunais pátrios e Cortes Superiores, e aplicado nestes casos.

Muitas das análises trazidas pela posição jurisprudencial são no sentido de identificar a quebra da cadeia de custódia como uma indiscutível mácula ao curso do processo penal[103], e que apesar de serem passíveis de declaração de nulidade, devem obedecer a via cognitiva adequada, restando um questionamento a se fazer, acerca da volumosa e desnecessária movimentação processual gerada pelas proposituras de novas demandas a cada dia, diante da ausência de posicionamento que fixe um termo para análise dos recursos até então pendentes, ou realizando o emprego de técnicas de superação de entendimento jurisprudencial, ou até mesmo edição de novas súmulas que tratem do tema, dando regramento provisório até que se estabeleça posição normativa consolidada.

Em certos contextos, tem-se que grande parte dos processos que visam discutir o tema, sob o prisma do reconhecimento de eventual nulidade contida no processo, costuma esbarrar em alguma ocasião de reanálise de contexto fático probatório, sendo aplicado entendimento de que processualmente falando não se tornaria viável a discussão de tais elementos se não no curso da via cognitiva.

O entendimento acerca da imprescindibilidade da existência de códigos hash íntegros, do momento de sua extração para análise investigativa, tem-se posicionamento já firmado pelo Superior Tribunal de Justiça, no sentido de trazer o ônus ao ente estatal, no cumprimento dos requisitos de garantia da integridade do material digital colhido na investigação, sob pena de nulidade da prova ali contida ou dela derivada, reconhecendo assim o rompimento da cadeia de custódia digital, bem como a contaminação dos dados contidos. É o que se mostra claro do julgado do RHC 143.169/RJ[104], de relatoria do excelentíssimo Senhor Ministro Messod Azulay, valendo realizar destaque ao ônus estatal para a comprovação da integridade do material colhido.

Diante destes entendimentos resta suscitar uma questão; será que diante de uma nulidade gritante no curso de uma investigação criminal, a qual é preliminar até mesmo o próprio processo cognitivo, encontrada em já fase recursal ulterior, esta não pode ser suscitada

---

[103] **STJ, RHC 77.86/PA, rel. Min. Ribeiro Dantas, julgado em 05.02.2019, publicado *in* DJ-e em 12.02.2019.**

[104] **STJ, AgRg no RHC 143.169/RJ, rel. Min. Messod Azulay, rel. para acórdão Min. Ribeiro Dantas, julgado em 07.02.2023, publicado *in* DJ-E em 01.03.2023.**

em via própria para tal, como é a via mandamental? Se não esta a via adequada para tratar do tema, e já esgotadas as vias cognitivas, qual será a via eleita a mais compatível para enfrentamento do incidente processual a ser questionado? Será que não pode mais levantar tal prejuízo o investigado afetado por tal nulidade? Pode um investigado, ser prejudicado por uma falta de esgotamento nas vias próprias, diante de uma nulidade absoluta, como é o caso de uma declaração de prova digital violada, alterada ou modificada? Já não é tempo de tomada de uma decisão mais detalhada e abrangente sobre o tema por parte dos órgãos do Poder Judiciário?

Ficam tais questionamentos levantados para discussões futuras, tanto nos meios acadêmicos, de modo que fomentem o debate temático, quanto até mesmo para futuras decisões dos Tribunais e Cortes Superiores.

4.2 Meios de violação e técnicas digitais antiforense e raciocínios pertinentes.

Ao mesmo passo que os profissionais da atividade forense digital precisam se adaptar às inovações tecnológicas trazidas pela disponibilização de serviços como "*Cloud Storage*", aqueles que detêm capacidade técnica para realizar sabotagens à estes sistemas e serviços também exercem as atividades antiforenses com o intuito de inviabilizar o acesso à estas plataformas de "*Cloud Computing*", ou até mesmo das informações e dados digitais ali contidos.

Aqui deve se fazer um adendo, no sentido de que, a utilização de técnicas e atividades antiforenses também podem ser utilizadas por indivíduos de boa-fé, buscando o sigilo de informações que seriam prejudiciais à eles ou aos interesses de determinadas entidades e instituições. Veja conforme:

> [...]
> As técnicas antiforenses podem ser empregadas por vários usuários para diferentes fins: além de serem usadas por grupos criminosos e terroristas, elas são utilizadas para o bem por entidades (organizacionais ou individuais) que desejam manter sua privacidade online e/ou destruir seus dados privados seguramente. (HASSAN, 2019, p. 163).
> [...]

Hassan[105] também afirma que a utilização de técnicas antiforenses envolvem muitos aspectos da segurança de computadores, estando o investigador forense digital sujeito a se deparar com situações de "1. Técnicas de ocultação de dados (conhecida como esteganografia);

[105] Parte das críticas trazidas pelo movimento técnico-científico, que lida com a perícia forense digital, traz os levantamentos acerca das técnicas antiforenses que são enfrentadas no cotidiano de um agente investigativo, bem como os elementos necessários à realização desta atividade pericial – **v. cf. HASSAN, 2019, p. 263.**

2. Técnicas de destruição de dados (antirrecuperação); 3. Técnicas de criptografia; 4. Técnicas criptográficas de anonimato; 5. Ataques diretos contra ferramentas de computação forense".

Realizando uma correlação entre os aspectos ligados às práticas antiforenses digitais e os institutos do Direito Digital e Informático, Direito Penal e Processual Penal, tem-se que algumas das técnicas empregadas serão no intuito de tentar embarreirar de alguma maneira a configuração aos elementos de autoria, materialidade e punibilidade, como já visto anteriormente, trazendo assim algumas críticas pertinentes.

Voltando-se à autoria, claramente se verifica uma questão quanto à exatidão de identificação da autoria, como já demonstrado, algumas das práticas serão no sentido de camuflar a identidade do indivíduo, que se valeu de determinado dispositivo eletrônico para o cometimento de ilícito, não bastando assim então a mera identificação o aparelho que foi utilizado; aqui vale a ressalva quanto à constatação estar limitada apenas à qual seriam os dispositivos envolvidos em determinada troca de informações, dado ou metadado, restando ainda apurar as demais conjecturas para possibilitar o ensejo de determinadas medidas contra o indivíduo[106], como é o caso de uma investigação realizada através de ente público estatal e posteriormente de ensejo à uma persecução criminal.

Este é o ponto central de partida para compreensão de até onde os limites estatais podem alcançar eficácia frente os mecanismos normativos vigentes, da mesma forma é o ponto central para entender quais as garantias mínimas que os indivíduos podem se valer para fazer prevalecer seus direitos e resguardos em suas esferas jurídicas pessoais.

Neste momento residem algumas breves implicações jurídicas que devem ser levantadas posteriormente à explanação dos demais conceitos técnico-científicos, os quais envolvem a discussão temática sob uma perspectiva da tecnologia da informação e do uso dos dados digitais.

A primeira delas é justamente a delimitação de quem seria o agente específico que estaria no controle de determinado dispositivo em determinado momento, e sob quais condições e circunstâncias tal agente estaria realizando a troca de determinada informação, dado ou metadado, o que acabaria por trazer implicações quanto à negação de autoria e materialidade de determinado fato considerado como antijurídico, e que poderia acabar por gerar ineficiência da atividade jurisdicional realizada de forma equivocada. Neste sentido explica:

> [...]
>
> Não basta apontar a máquina da qual partiu o comando, é preciso precisar quem operava o aparato no momento da conduta. E não basta apenas

[106] Problema de relativização da autoria, trazido pelo movimento doutrinário como uma crítica a ser enfrentada na fase investigativa – **v. cf. SYDOW, 2022, p. 327-328.**

> tal precisão de modo automático: é preciso eliminar as hipóteses de presunção técnica de afastamento ou relativização de autoria. (SYDOW, 2022, p. 121). [...]

Derivado deste pensamento, extraem-se algumas considerações principiológicas específicas das áreas de atuação do Direito Digital, a mero título de exemplo pode-se trazer o Princípio da Dupla Presunção de Inocência, que traz consigo uma consideração de extrema relevância ao afastamento desta negação de autoria, que reside exatamente na fragilidade de identificação de autoria e materialidade apenas por identificação de endereço de IP, restando assim a chamada por Sydow de "IMPRECISÃO DE AUTORIA que se pode dar por defeito na composição da identidade ou por manipulação da autoria (própria ou por terceiro)"[107].

Fora deste cenário, ainda que se restasse certa e precisa a autoria do indivíduo cometedor do ilícito, como já destacado, as circunstâncias em que se realizou o cometimento de tal ato também deve ser analisada, pois pode claramente o indivíduo estar no cometimento de um ilícito sob influência de uma coação, sendo ela física ou moral irresistível[108], igualmente pode estar realizando tal ilícito por motivo de alta relevância social[109], aqui também já se fazendo alusão aos elementos da punibilidade.

Não aversa à esta realidade, tem-se que a existência de práticas de *hacking*[110] são muito comuns, de modo que os próprios tribunais pátrios já sofreram com tentativas de invasões externas. *Hacking* são práticas que se utilizam de invasão ao sistema operacional, na tentativa de corrompimento, edição, modificação, alteração ou exclusão de alguma informação, através de um dispositivo eletrônico externo à rede utilizada, criando assim uma brecha naquele determinado sistema operacional.

Aqui se falando então das técnicas de "*ataque direto contra as ferramentas de computação forense digital*"[111], assim como também das técnicas de antirrecuperação[112] e técnicas de criptografia[113].

Claramente se mostra a necessidade de atenção à tais condutas, bem como a modificação de algumas práticas, na tentativa de blindar todo e qualquer sistema operacional

---

[107] Conceito trazido para demonstrar a fragilidade entre o sistema investigativo, no que tange às práticas empregadas para cometimento de ilícitos, se utilizando de dispositivos eletrônicos – **v. cf. SYDOW, 2022, p. 118.**

[108] Imposição de uma das causas excludentes de culpabilidade, como é o caso da coação física, onde o usuário do dispositivo eletrônico estaria sob forte pressão física, para realizar o cometimento do ilícito através do meio digital; raciocínio explorado pela doutrina do Direito Digital e Informático ao analisar a figura da coação como excludente de culpabilidade – **v. cf. SYDOW, 2022, p. 385-386.**

[109] Raciocínio realizado no sentido de não trazer alguma causa de isenção de pena, mas que claramente iria incidir sobre fases da dosimetria de pena, nos termos da alínea *a*, do inciso III, do art. 65, Código Penal – v. cf. **BRASIL. Decreto Lei nº 2.848, de 1940, institui o Código Penal Brasileiro. 3 jan. 1941.**

[110] Conceito trazido pela Tecnologia da Informação para as práticas utilizadas pelos indivíduos *hackers* – **v. cf. SYDOW, 2022, p. 330.**

[111] Técnicas utilizadas pelos agentes das áreas relacionadas a perícia forense digital, utilizadas em seu cotidiano – **v. cf. HASSAN, 2019, p. 278.**

[112] **Op. Cit. p. 269.**

[113] **Op. Cit. p. 273.**

utilizado pelo estado no curso das investigações criminais, bem como dos processos judiciais em curso.

Faz-se necessário ressaltar novamente acerca das características inerentes aos dados e metadados digitais, de modo que a volatilidade e incerteza quanto à figura do usuário do dispositivo eletrônico no momento do cometimento do ilícito, conforme ressalta Sydow:

> [...]
> Enfim, as relações informáticas têm como característica fundamental, por ocorrerem através de aparatos, a falta de certeza absoluta acerca das características do usuário infrator, levando a uma dificuldade imediata de identificação do autor dos atos delituosos eventualmente ocorridos. (SYDOW, 2022, p. 313).
> [...]

Além das situações de tentativa de invasão aos sistemas operacionais, causando corrompimento de dados e de informações contidas e utilizadas ao longo dos processos criminais, tem-se também as ocasiões de camuflagem de evidência digital, ou de fragmentação desta, por meio de técnicas de ocultação de dados[114], que consistem no mascaramento de determinada evidência em meio à um dado ou metadado digital diverso do investigado, deixando assim um rastro digital muito mais complexo de ser alcançado pelos peritos investigativos.

Todos esses elementos devem ser considerados, no momento da subjunção de todas as diferentes perspectivas do caso concreto, a fim de trazer maior garantia ao procedimento investigativo, ao processo penal, bem como ao indivíduo investigado e processado e ao aparato estatal mobilizado.

Todas estas condições devem ser calma e friamente analisadas, bem ponderadas e posteriormente bem postas, uma a uma, desde o procedimento investigativo empregado, passando por toda a etapa de perícia forense digital explanada nos tópicos anteriores, até mesmo o processamento e devido tratamento de cada um dos materiais, informações, dados e metadados digitais colhidos e contidos na persecução penal, perfazendo assim toda a cadeia de custódia digital e a devida instrumentalização de todas as evidências no curso do processo.

4.3 Dispositivos normativos, tratados internacionais e jurisprudência existente que versa sobre o tema.

[114] Também chamadas de esteganografia digital – v. cf**. Hassan, Nihad A. Perícia Forense Digital. p. 264, 2019.**

Em se tratando de produção de prova de natureza digital, haverá a necessidade de análise dos instrumentos normativos que compõe o nosso sistema jurídico processual, voltado à área de atuação do Direito Penal e do Direito Processual Penal, pode-se fazer as considerações quanto às codificações já existentes que versam sobre o assunto, bem como também as legislações que trazem abordagem temática pertinente ao uso de dados digitais como meio de prova.

Deve-se adentrar nos institutos específicos dos Código Penal e Código de Processo Penal, bem como os conteúdos normativos contidos nas legislações esparsas que formam o conjunto de regramentos aplicáveis aos casos de usabilidade de provas digitais, da sua necessidade para se valer de meio de prova, e claro, da sua validade como tal.

Para mera exemplificação das diversas normas vigentes que tratam de alguma forma sobre o uso de dados digitais nos processos em geral, pode-se citar a Lei Geral de Proteção de Dados-LGPD, a Convenção Internacional de Budapeste sobre os crimes cibernéticos, a Lei nº 12.965, de 2002, conhecida como a Lei do Marco Civil da Internet, as Lei nº 12.527, de 2011, conhecida como Lei de Acesso à Informação, bem como os comandos normativos contidos no Título VII, do Código de Processo Penal, que versam sobre as provas e os meios empregados quanto à estas.

Até mesmo as atividades legislativas estrangeiras devem ser analisadas, no intuito de trazer uma maior chance de sucesso na atividade normativa e legisladora dos nossos entes. Mas tal análise deve ser feita em momento oportuno, à posteriori e em subtópico específico.

Seguindo este raciocínio, há de se levantar a situação da atividade legislativa desempenhada nas últimas décadas, que pode ser tida como prova concreta desta "incompatibilidade de acompanhamento" da norma frente à necessidade da humanidade de evoluir e "simplificar" a vida cotidiana, ao passo que se demonstram as inovações legislativas quase que quinquenalmente no tocante à matéria de tecnologia e uso de dados digitais, a mero título de exemplo a própria Lei Geral de Proteção de Dados-LGPD, que traz a disciplina legal do uso dos dados somente veio a ocorrer em 2018, sendo que o chamado "marco civil da internet" no Brasil aconteceu em 2014.

De idêntica forma, deve-se levar em consideração que algumas das questões que trazem a situação de "desconformidade" ou de "disparidade" da realidade cotidiana para as problemáticas trazidas pelas aplicabilidades das normas atualmente vigentes, tem correlação direta com o monitoramento eletrônico e controle externo dos dados digitais[115],

[115] Fazendo-se menção à característica de manipulabilidade dos dados digitais – **v. cf. SYDOW, 2022, p. 310.** –, trazendo correlação com os dispositivos normativos contidos na Lei Geral de Proteção de Dados-LGPD, de modo que o adequado tratamento de dados deve ser realizado

problematização esta que somente tem sido enfrentada pela comunidade jurídica mais recentemente após o implemento da referida LGPD, bem como aos debates trazidos ao Poder Legislativo recentemente, pela necessidade de implementação também de uma LGPD Penal[116].

Diante desta desconformidade, claramente se mostra eficaz o levantamento ao debate acerca da posição jurisprudencial quanto à estes dispositivos, institutos do Direito Processual Penal, e até mesmo diante destas alterações legislativas. Passa-se à esta análise diante das diversas posições dos Tribunais e das Cortes Superiores.

Os Tribunais Regionais têm entendimentos um tanto quanto assimétricos acerca da aplicação da devida instrumentalização, de cada um dos procedimentos e suas etapas inerentes, para ser reconhecida a efetiva violação da cadeia de custódia da prova digital. Alguns precedentes diversos trarão mais clareza à esta figura. No caso do Tribunal Regional da Terceira Região-TRF3, tem-se uma clara demonstração deste cenário de assimetria.

Em certa medida é reconhecida a imprescindibilidade dos procedimentos para realização do uso da prova digital em nuvem na investigação criminal, porém, em certos pontos, algumas minúcias se mostram ainda não sanadas, como foi o caso do reconhecimento por parte do Tribunal que *o "Juízo de origem esclareceu com detalhes toda o desenrolar da questão. Após a defesa alegar falta de arquivos de mídia, a Policia Federal disponibilizou nova gravação em 17/03/2023 e 24/03/2023*." [117], deixando clara a falta de disponibilização integral dos arquivos por parte da autoridade investigativa, frente àquela etapa do procedimento, para com a defesa, ocasião em que a mesma impetrou ordem mandamental contra esta situação.

No presente exemplo em questão, se obteve resultado negativo, porém, de qualquer modo foi suscitada frente ao Poder Judiciário, demandando além da própria ação penal investigativa, por claramente faltar-lhe observância neste aspecto naquele momento, exigindo assim mais ainda do aparato estatal. Na ocasião foi trazido resultado negativo apenas sob o aspecto da ótica processual, devido o fundamento da "*análise do caminho percorrido na cadeia de custódia da prova é matéria que demanda inserção no contexto fático-probatório, medida incabível na via estreita do habeas corpus"*. [118]

Apesar de correta a decisão quanto ao caminho incorreto percorrido para a discussão da questão, claramente se deixou evidente uma situação de indisponibilidade acerca da

---

pelos agentes públicos adequadamente capacitados – **v. cf. ELEUTÉRIO; MACHADO, 2019, p. 26-27. –** também contida esta compreensão nas áreas da perícia forense digital – **v. cf. HASSAN, 2019, p. 98.**

[116] Projeto de Lei, que visa criar a Lei Geral de Proteção de Dados Penal, no intuito de trazer um melhor tratamento de dados pessoais, no que tange aos aspectos da criminalização de atos ilícitos – v. cf. **Projeto de Lei nº 1515, de 2022.**

[117] **TRF3, HC 5019314-16.2023.4.03.0000, rel. Des. Fed. Paulo Gustavo Guedes Fontes, julgado em 22.08.2023, publicado *in* DJ-e em 22.08.2023.**

[118] *Opus cit.*

integralidade do material colhido na investigação para com a figura da Defesa, o que levanta a discussão acerca do volume de demandas judiciais que se encontram em mesma situação, onde não seriam necessárias as enxurradas de impetrações de medidas assecuratórias do direito à liberdade do indivíduo, se tais minúcias procedimentais fossem esclarecidas ao longo da instrução criminal que realizou a própria investigação.

Em outra ocasião, o Tribunal Regional Federal da Primeira Região-TRF1 realizou a análise de uma impetração em sentido similar[119], e para definição da questão foram trazidos diversos outros elementos, vultuosa prova documental e pericial do material apreendido, relevante prova testemunhal e verificação de múltiplos fatores, utilizados pela autoridade investigativa, os quais pudessem serem utilizados como fundamentos capazes de corroborar o conteúdo da prova digital supostamente violada, pois senão teria ocorrido um cenário de nulidade clara.

São alguns casos dentre milhares nos Tribunais pátrios, que têm sido demandados em razão de uma ausência de esgotamento da discussão acerca da cadeia de custódia digital nas fases preliminares ao processo, ou até mesmo iniciais a ele. Crê-se fortemente na necessidade de implementação de uma cultura de enfrentamento minucioso ao tema, levando em conta todas as perspectivas.

Também soa compatível tal raciocínio com o entendimento aplicado pelo Superior Tribunal de Justiça quando afirma que *"É ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia."*[120]. E destaca:

> [...]
> No processo penal, a atividade do Estado é o objeto do controle de legalidade, e não o parâmetro do controle; isto é, cabe ao Judiciário controlar a atuação do Estado-acusação a partir do direito, e não a partir de uma autoproclamada confiança que o Estado-acusação deposita em si mesmo. (STJ, 5ª Turma, AgRg no RHC 143.169/RJ, rel. Min. Messod Azulay, rel. acórdão Min. Ribeiro Dantas, julgado em 07.02.2023, publicado *in* DJ-e em 01.03.2023).
> [...]

O caso toma ainda maiores delineamentos quando se trata de matéria voltada à quebra da cadeia de custódia da prova digital contida em dispositivos de nuvem, WhatsappWeb no

[119] **TRF1, HC 1033633-48.2022.4.01.0000, rel. Des. Fed. Ney Belo, julgado em 13.10.2022, publicado *in* DJ-e em 13.10.2022.**
[120] **STJ, 5ª Turma, AgRg no RHC 143.169/RJ, rel. Min. Messod Azulay, rel. acórdão Min. Ribeiro Dantas, julgado em 07.02.2023, publicado in DJ-e em 01.03.2023.**

caso, mostrando-se clara a volatilidade[121] dos dados apresentada, de modo que se declarar a a natureza e característica de *"não deixar absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, não pode jamais ser recuperada para efeitos de prova em processo penal"* [122], não sendo assim viável sua utilização como meio de prova no processo penal. Tal posição foi recentemente reconfirmada trazendo entendimento pela invalidade da prova assim produzida.[123]

Ainda neste entendimento, além da autenticidade do material extraído, da necessidade de acompanhamento das etapas do procedimento investigativo, a fim de garantir a integridade do material apreendido, se mostra também posicionado o entendimento jurisprudencial da Corte Superior de Justiça[124], no sentido de trazer a imperiosidade da devida disponibilização integral destes conteúdos, sem qualquer tipo de mácula, alteração ou modificação para a contraparte, de modo que qualquer óbice ou instabilidade desta ocasião gera nulidade pela perspectiva do cerceamento de defesa e do malferimento ao princípio da paridade das partes[125].

Como pode-se notar, além de ser um cenário relativamente novo para o contexto dos Tribunais e Cortes Superiores do país, é também uma ocasião em que se têm cognição de muitos elementos novos já em fase avançada dos processos penais, de modo que se mostraria proveitoso um posicionamento mais ostensivo por parte do Poder Judiciário e seus órgãos, bem enquanto não se mobilizam os entes legiferantes com mais especificidade sobre o tema.

Pode também ser realizada por parte do Poder Judiciário alguma técnica de *overruling*[126], diante das diversas teses apresentadas perante os tribunais pátrios que tratam do tema, as quais ainda estão pendente de julgamento, ou até mesmo algum tipo de modulação de efeitos relativos à demandas repetitivas, e casos em regime de repercussão geral diante de sua relevância jurídica contemporânea.

4.3.1 Uma breve síntese das experiências dos Estados estrangeiros e uma análise do direito comparado.

[121] Característica trazida pela Tecnologia da Informação ao correlacionar com dados digitais – v. cf. **OLIVEIRA, Vinícius Machado. Identificação, coleta, aquisição e preservação da evidência. 2018.**

[122] **STJ, 6ª Turma, RHC 99.735/SC, rel. Min. Laurita Vaz, julgado em 27.11.2018, publicado *in* DJ-e em 12.12.2018.**

[123] **STJ, 6ª Turma, AgRg no RHC 133.430/PE, rel. Min. Nefi Cordeiro, julgado em 23.02.2021, publicado *in* DJ-e em 26.02.2021.**

[124] **STJ, AgRG no HC 735.027/SP, rel. Min. Sebastião Reis Júnior, julgado em 26.09.2023, publicado *in* DJ-e em 04.10.2023.**

[125] Princípio norteador do Direito Processual, que pode ter aplicabilidade nos ramos do Direito Processual Penal, com direta conexão com os institutos do contraditório e da ampla defesa – **v. cf. SILVA, Naiara Lisboa. 2018, pg 4-6.**

[126] Conceito processual trazido para superação de entendimentos firmados em sede de súmula ou julgamento de demandas repetitivas – **v. cf. GOMES, Rodolfo Perini. 2019, p. 33.**

Além da perspectiva normativa e legislativa pátria, tem-se também uma breve análise de institutos do direito comparado para personificar melhor as críticas feitas à toda esta temática. Para trazer uma maior clareza quanto aos meios que podem ser seguidos pelas entidades e organismos legiferantes do estado brasileiro, tem-se as experiências realizadas pelas nações europeias, que conjuntamente empenham esforços para enfrentamento do tratamento adequado de dados digitais há mais tempo.

Notavelmente a comunidade internacional aborda o tratamento de dados digitais com o devido cuidado desde a década de 80, quando foi realizado a Convenção para Proteção dos Indivíduos com respeito ao Processamento Automático de Dados Pessoais[127], que foi alterada pela Diretiva 95/46/EC[128], do Conselho Europeu, a qual veio a trazer a proteção e o direito de resguardo aos dados digitais pessoais dos indivíduos, bem como o livre tratamento dos dados digitais.

Posteriormente, houve a realização e a edição da Convenção Internacional de Budapeste sobre Cybercrimes[129], realizada em 2001, a qual veio trazer a devida abordagem aos crimes realizados em meios virtuais, bem como trouxe o devido regramento e disciplina acerca das obrigações e deveres de cada estado membro, no tocante à necessidade de repressão à tais condutas, bem como o compartilhamento de informações que auxiliem os estados membros nesta efetiva reprimenda.

Seguindo neste alinhamento, e tendo como um belo exemplo a ser seguido, a atividade das entidades legislativas germânicas vêm trazendo o devido regramento ao tratamento de dados digitais dos indivíduos desde a década de 70, quando promulgou em 1979 o *Bundesdatenschutzgesetz-BDSG*[130], legislação alemã que é similar à nossa Lei Geral de Proteção de Dados-LGPD, mas com o advento de que naquela legislação estrangeira já ocorreram até mesmo alterações normativas, que fossem compatíveis com os demais regramentos realizados pelo Conselho da Europa sobre os temas.

Igualmente ocorre nas nações da Itália e Espanha, que tem seus regramentos desde 2001 e 2016, sendo estes o *Codice in Materia di Protezione Dei Dati Personali*[131] e a *Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales*[132]

---

[127] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – v. cf. **Council of Europe Convention No. 108 on data protection.**

[128] Directive 95/46/EC of the European Parlament and of the Council of 24 October 1995, on the Protection of Individuals With Regard to the Processing of Personal Pata and on the free movement of such data - v. cf. **EC/46/95**.

[129] **Convention on Cybercrime Budapest. Council of Europe Convention. Nov. 2001.**

[130] **Bundesdatenschutzgesetz. Jun. 2017.**

[131] **Codice In Materia Di Protezione Dei Dati Personali. Legge Delega nº 127. 2001**.

[132] **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.**

respectivamente, sendo que a própria legislação espanhola também já sofreu alterações em sua redação para a compatibilização das realidades vivenciadas no contexto da digitalização dos dados pessoais, bem como dos meios de cometimento de ilícitos através de meios e instrumentos digitais.

Está mais que esclarecido que a comunidade internacional já enfrentou o tema com mais seriedade, a ponto de alcançar diversas possíveis soluções que podem ser adaptadas à realidade do cenário da atividade estatal brasileira, principalmente para com o Poder Judiciário e Poder Legislativo. Podem os organismos e entes legiferantes brasileiros realizar uma análise, com intuito de adequar o que pode ou não funcionar na realidade da atividade jurisdicional pátria, visando alcançar o sistema mais eficiente para implementação e enfrentamento do tema.

Esta é uma crítica que deve ser amplamente explorada pelos futuros estudiosos do tema, principalmente no intuito de auxiliar no avanço das discussões temáticas e da edição de normas compatíveis com o devido tratamento de dados digitais e a respectiva cadeia de custódia digital anteriormente explanada.

4.4 A devida procedimentalização e utilização dos dados digitais e dados digitais em nuvem no processo criminal.

Já está mais que esclarecido a necessidade na observância das especificidades da prova digital, bem como dos mecanismos de tratamento do dado e metadado digital em nuvem, e tendo sido esclarecidas as questões relativas aos procedimentos e técnicas atualmente empregadas, bem como uma breve análise dos precedentes citados e das experiências comparadas, se vê que um exame mais delicado da adequada instrumentalização pode auxiliar os demais raciocínios conclusivos, acerca da realidade enfrentada e de possíveis caminhos a serem seguidos, bem como de uma viabilização de futuros debates técnicos.

Voltando ao debate mais construtivo acerca do tema, algumas das perspectivas abordadas e dos raciocínios apresentados levarão à um possível entendimento, sobre a necessidade de edição e promulgação de novas legislações que acabem por trazer uma melhor adequação normativa às situações fáticas cotidianas que envolvem o contexto dos dados digitais e do uso destes dados como meios de se fazer atividade jurisdicional sem malferir os direitos e garantias mínimas da população.

De idêntica forma alguns raciocínios irão levar à um possível entendimento sobre a possibilidade de adaptação dos procedimentos, técnicas e métodos já existentes de coleta e

utilização destes dados digitais para se fazer desta atividade jurisdicional, o que ocasionará um enorme dispêndio estatal para com seus agentes, conforme se extrai de Souza:

> [...]
>
> Haverá, principalmente nos primeiros anos de vigência dessas recentes regras de custódia de provas, muitos contratempos vinculados à falta de treinamento das pessoas encarregadas em atuar em cada uma das fases previstas no art. 158-B do CPP, além da ausência de recursos humanos e financeiros para viabilizar os recursos materiais indispensáveis para o cumprimento dos protocolos criados, principalmente no âmbito dos departamentos de polícia técnico-científica dos Estados, desde já sendo possível prever a existência de significativo número de questionamentos acerca do descumprimento de uma ou mais das etapas da cadeia de custódia, desde já sendo relevante afirmar que o eventual descumprimento irá constituir mera irregularidade, não gerando a nulidade das provas respectivas, exceto quando ficar demonstrado o efetivo comprometimento da integridade da cadeia de custódia, a ponto de gerar dúvidas concretas quanto à adulteração, substituição ou contaminação dos vestígios apreendidos, inviabilizando a necessária confiança no resultado da perícia, ou mesmo inviabilizar a realização do exame pericial (SOUZA, 2020, p. 197).
>
> [...]

Porém deverão ocorrer algumas ressalvas quanto à estas adaptações, que deverão ser realizadas com muita segurança, e principalmente, muita perícia e maestria, de modo a evitar o mesmo malferimento que poderia ocorrer caso viesse a ser realizada edição e promulgação de novos comandos normativos que fossem igualmente desrespeitados pelos operadores destas atividades estatais já existentes na forma e modo que existem.

Algumas das perspectivas apresentadas trazem um sentido mais restrito à atividade estatal, que será por vezes pormenorizada e criticada ao realizar os procedimentos adequados previstos nas legislações vigentes atualmente. É o caso das críticas voltadas ao excesso de brechas deixada pelo sistema normativo vigente, sofrendo uma mera adaptação para compatibilizar com mecanismos digitais e virtualizados, tendo assim ausência de legislação específica para tal.

Neste sentido os estudiosos da perícia digital forense trazem a compreensão acerca da estrutura física e o aparato necessário para a melhor realização das atividades investigativas periciais voltadas à análise de dados e metadados digitais, assim como os contidos em dispositivos de *Cloudstorage*.

Além de material humano e de equipamentos compatíveis com a atividade investigativa forense digital, é necessário um respeito à diversos requisitos para compor uma unidade de tratamento de dados digitais com fins periciais, sendo inclusive defendido por parte

de profissionais da área a possibilidade de criação de unidades de *compliance*[133] para realização de auxílio da prática investigativa forense, com fins de atividade probatória para com o ente estatal, de modo a demonstrar seus benefícios à prática investigativa, seguindo seus regramentos voltados à instituição de um ente vinculado à fiscalização do indivíduo parceiro do Estado.

Este raciocínio se mostra também em Hassan[134], relativo à uma experiência comparada, demonstrando a possibilidade de investigação conjunta entre o Estado e corporações voltadas para este fim; afirma-se ainda acerca da estrutura necessária para um laboratório pericial forense, e neste ponto destaca a imperiosidade da criação de cada uma das estruturas com seu controle de ambiente[135], fornecimento de cada um dos materiais de *hardware*[136], construção de uma sala de evidência[137] com suas respectivas estruturas, obtenção dos programas de *softwares*[138] e capacitação dos profissionais[139], e uma devida certificação[140] para alcance da medida investigativa adequada.

É o que se extrai sobre os requisitos das instalações físicas de uma unidade investigativa pericial forense digital, nota-se: *sic*

> [...]
>
> Os requisitos físicos básicos a seguir são altamente prioritários em qualquer laboratório forense digital:
>
> 1. Deve ter uma única porta de entrada.
> 2. É preferível que não tenha janelas.
> 3. O laboratório deve ser à prova de som, o que significa que ninguém deve ser capaz de escutar ocultamente as conversas que ocorrem dentro dele. É possível conseguir isso com o uso de material à prova de som no teto e nas paredes bem como carpete no chão.
> 4. Deve ter um sistema de alarme na entrada, além de um sistema biométrico para manipular o acesso. O sistema biométrico de acesso deve registrar cada visita ao laboratório; esse log deve permanecer em backup por muitos anos para fins de auditoria.
> 5. Câmeras de vigilância devem cobrir o laboratório inteiro, principalmente a entrada principal e a sala de evidência digital. O gravador de vídeo do sistema de vigilância (onde os arquivos de gravação em vídeo são armazenados) deve ser guardado na sala mais segura do laboratório, ou seja, a "sala de armazenamento de evidência".
> 6. Deve ter sistemas de extinção de incêndio. (HASSAN, 2019, p. 84-85).
>
> [...]

---

[133] Thamay e Tamer trazem os conceitos de uma atividade de *compliance* para atividade probatória em conjunto com o Estado, na tentativa de sanar parte das dificuldades investigativas – **v.cf. THAMAY; TAMER. 2022, p. 106-109.**

[134] Considerações de Hassan sobre a experiência dos Estados Unidos e atividade investigativa em laboratórios privados, bem como suas necessidades e especificidades como local de atividade laboral investigativa forense digital – **v. cf. HASSAN. 2019, p. 82.**

[135] ***Op. Cit. p. 86.***

[136] ***Op. Cit. p. 87.***

[137] ***Op. Cit. p. 89-90.***

[138] ***Op. Cit. p. 92***

[139] ***Op. Cit. p. 95, p. 98.***

[140] ***Op. Cit. p. 100-102.***

E completa ainda trazendo uma planta exemplificativa acerca do design sugerido para um laboratório forense digital, afirmando ser o mais "*apropriado para grandes organizações privadas e governamentais"*[141]. Ultrapassada a compreensão preliminar sobre a necessidade de instalações adequadas para o tratamento do dado e metadado digital, volta-se ao procedimento investigativo forense adequado, que tem identicamente sua altíssima importância.

Conforme exaustivamente demonstrado nos tópicos anteriores, bem como no capítulo anterior, há uma necessidade de observância criteriosa de cada uma das etapas de procedimentalização da informação contida em determinado meio digital, seja ele qual for, desde dados e metadados digitais contidos em dispositivos eletrônicos móveis até mesmo os dados contidos em sistemas de armazenamento em nuvem; desta forma uma explanação breve acerca do procedimento de instrumentalização do dado digital, o qual se faz crer ser o mais adequado à realidade factual constantemente mutável, parece viável. Passa-se à tal raciocínio.

Por primeira etapa se faz inerente e clara a identificação de um delito cometido através de meios digitais, ou se fazendo valer destes meios para resguardar determinada informação utilizada no cometimento do delito em si. Este intuito nos trará a compreensão acerca da utilidade do determinado dado digital, contido ou não em nuvem ou dispositivo móvel, como uma prova em seu fim ou como um meio de obtenção para tal. A corrente doutrinária processual se mostra posicionada neste sentido[142].

Por etapa posterior à identificação do delito com intrínseca relação com os meios digitais, passa-se à etapa de alcance, em conjunto com o provedor de rede[143], das informações relativas ao endereço de IP, com a finalidade de localização de uma das etapas procedimentais de interligação com a autoria do individuo que esteja naquele momento utilizando aquele meio digital para o cometimento do ilícito penal. Ao ter acesso à esta informação parcial, passa-se à uma etapa de realização de diligência e alcance, ao menos momentaneamente e de forma preliminar, do dispositivo eletrônico utilizado para o alcance da fase de consumação do *iter criminis*.[144]

Parece ser simples a realização da diligência com fins de obtenção do aparelho eletrônico utilizado, mas não é. Alguns raciocínios se mostram necessários para a adequada posse do dispositivo eletrônico utilizado no ilícito penal.

---

[141] ***Op. Cit. p. 84-85.***

[142] Entendimento jurisprudencial citado – **v. cf. AURY, 2023, p. 426; SOUZA, 2020, p. 37-38.**

[143] Neste sentido é trazido pela corrente doutrinária respectiva – **v. cf. ELEUTÉRIO; MACHADO, 2019, p. 108-109.**

[144] Traz as etapas do *iter criminis*, tendo como premissa a consumação **- SYDOW, 2022, p. 329; NUCCI, 2022, p. 252-253.**

Uma vez na posse do dispositivo eletrônico utilizado, entram os questionamentos relativos à imprecisão de autoria[145], as quais, conforme também esclarecido supra, devem ser superadas pela verificação de múltiplas etapas[146] do dispositivo eletrônico periciado.

Mas ora, como realizar a verificação de um fator de múltiplas camadas sendo que o dispositivo, o qual necessita estar na posse do seu usuário para autenticação, já se encontra devidamente apreendido e custodiado pela central de análise forense?! Já se encontra inviabilizada esta etapa de forma posterior à obtenção do dispositivo por parte da autoridade investigativa. Aqui surge um primeiro ponto a ser sanado quanto à realização da diligência para obtenção do dispositivo eletrônico utilizado.

A sugestão então seria que no momento do contato de realização do provedor de rede, para alcance das informações do usuário e realização de diligência, seja também conferido junto ao provedor de rede se o dispositivo eletrônico investigado já realizou algum procedimento de múltiplas camadas de autenticação recentemente, e tal informação pode ser obtida por parte dos provedores de rede; inclusive através de mecanismos já utilizados pelas próprias plataformas digitais destes mesmos provedores, quando do momento da contratação por parte do usuário, ou do acionamento da plataforma para uma central de atendimento ao cliente, é o caso das empresas de telefonia que servem como provedoras de suas próprias plataformas.

Ou seja, os próprios provedores de rede já detêm mecanismos de múltiplas camadas de autenticação, as quais já são utilizados pelos usuários de forma periódica ou esporádica em suas plataformas próprias, de modo que seja possível demonstrar que aquele determinado indivíduo é ou era o usuário daquele determinado dispositivo eletrônico, naquele determinado momento em que foi cometido o ilícito penal. É uma etapa de autenticação essencial, que causa um dispêndio inicialmente maior para a etapa investigativa, mas que traria uma grande economia aos andamentos processuais, reduzindo assim situações de imprecisão de autoria ou imprecisão de materialidade delitiva.[147]

O pensamento aqui se encontra viável de aplicação no cenário atual e também entra em congruência com o princípio da presunção de inocência[148], bem como o da dupla presunção de inocência[149], no sentido de estipular que ao menos momentaneamente, enquanto não são

---

[145] Ocasião em que é gerada "*uma segunda presunção de inocência, denominada TÉCNICA"* – **v. cf. SYDOW, 2022, p. 118.**

[146] **Op. Cit. p. 119.**

[147] Neste sentido a compreensão trazida por Sydow, no tocante à imprecisão de autoria, é aplicada conjuntamente com os entendimentos de Nucci, acerca da "culpabilidade material", quando se refere à inexistência de óbices para alcance da materialidade objetiva e dolosa do indivíduo cometedor de ilícito penal – **v. cf. SYDOW, 2019, p. 118; NUCCI. Manual de Direito Penal. 2022, p. 228.**

[148] Princípio norteador do Direito Processual Penal, amplamente defendido pela doutrina, que, neste contexto, tem o sentido de trazer as garantias de imperiosa observância para com os direitos do indivíduo investigado em uma ação penal – **v. cf. NUCCI. Provas no Processo Penal. 2022, p. 4-5; RENATO, 2021, p. 48; LOPES JR., 2023, p. 428; SOUZA, 2020, P. 122.**

[149] Diante da "manipulação da autoria" – **v. cf. SYDOW, 2022, p. 118 –** e da chamada "fragilidade TECNICA", ligada aos elementos da autoria, tem-se então a ocasião de dupla presunção de inocência **– v. cf. SYDOW, 2022, p. 119.**

obtidas as informações preliminares junto ao provedor de rede, para os fins de realização de uma diligência investigativa adequada e consistente, que aquele determinado indivíduo, cujo pode estar apenas na posse de determinado dispositivo, o qual já foi utilizado para cometimento de ilícito, ainda não pode ser considerado como o suspeito de ter enfim cometido aquele determinado ilícito.

Isto pois momentaneamente não se detém informações relativas à sua autoria, pelo menos enquanto não se verificar a autenticidade desta perante os métodos de identificação de múltiplos fatores, é um momento procedimental e processual em que se tem uma garantia aos princípios citados. Este pensamento é corroborado por Sydow.[150]

Tendo como premissa a característica da anonimidade está diretamente relacionada com a identificação dos usuários de meios digitais para cometimento de ilícitos, bem como daqueles que somente se valem desses meios para armazenamento de informações altamente incriminatórias, ou até mesmo sua alteração, modificação, disseminação e destruição, devido a sua fácil mobilidade e utilização. É a característica inerente à figura da autoria de determinado fato antijurídico, e que nela em si residem diversas fragilidades, devido sua natureza identicamente volátil.

Como se pode notar, a identificação de autoria no campo virtual depende de uma situação de presunção quanto à determinação do sujeito virtual que está se valendo daquele determinado dispositivo, para manipulação e manuseio daquele determinado dado ou metadado digital. Este é o pensamento trazido por Sydow:

> [...]
>
> Por conta de potencialmente qualquer pessoa poder utilizar a tecnologia informática, surgiu a insegurança no que se refere ao usuário conectado, que não possui em regra identidade pessoal, mas tão só uma identidade presumida, através da máquina conectada ou de uma conta criada.
>
> [...]
>
> Esta identificação presumida feita com base nos dados informados por cada usuário, ou presumida por um número de IP de um dispositivo, gerou o fenômeno da anonimidade relativa.
>
> Por anonimidade virtual, entende-se a falta de certeza quanto à identidade imediata referente a um usuário, levando-se em conta a impossibilidade de se atribuir o uso de um maquinário informático a uma pessoa determinada. (SYDOW, 2022, p. 312).
>
> [...]

Uma vez tendo sido ultrapassada esta etapa e devidamente realizada a diligência, bem como a identificação do IP do aparelho utilizado no cometimento do ilícito, bem como do autor precisamente verificado, tem-se enfim a etapa de obtenção do dispositivo.

---

[150] *Multiple steps of verification procedures* – **v. cf. SYDOW, 2022, p. 119.**

Apesar de enfim alcançada, deve-se observar os demais procedimentos da cadeia de custódia digital[151] tal qual seria com uma prova convencional, desde a coleta[152], acondicionamento e transporte[153], armazenamento[154], isolamento do material pertinente a ser periciado[155], extração de códigos hash do material[156], cópia do material por meio de backup[157], análise do material objeto da perícia[158], elaboração de relatório final de laudo pericial[159], e posteriormente ao termino da instrução criminal o descarte adequado destes dados e informações[160]. Cada uma destas etapas é de imperiosa observância.

Fora as etapas acima descritas, se necessário, deve ainda ser realizado, antes da extração do código hash da informação digital, uma outra etapa de descriptografia[161] ou outra medida similar compatível, para superar determinadas práticas antiforenses[162] desempenhadas pelos sujeitos destes ilícitos penais digitalizados. E algumas destas técnicas de descriptografia podem não obter êxito no alcance da senha de liberação do dado; mais uma dificuldade enfrentada pelos profissionais da seara da perícia forense digital.

A extração de código hash de determinada informação digital se mostra tão importante pois a quantificação[163] daquela informação, como já mostrado, trará a corroboração acerca da integridade do material coletado, restando assim as demais etapas do procedimento forense já resguardadas de muitas contaminações aos indícios, evidências ou provas ali contidas. Aqui se faz um adendo à importância da realização da cópia através de backup do arquivo original, contido no aparelho eletrônico apreendido, ambas as etapas, extração e cópia do material, caminham praticamente juntas.

---

[151] A perícia forense digital traz os elementares da cadeia de custódia digital, bem como seus requisitos – **v. cf. HASSAN, 2019, p. 42-43. –** pensamento corroborado pela doutrina do Direito Digital – **v. cf. SYDOW, 2022, p. 204-205; SOUZA, 2020, p. 194.**

[152] Trazida por Hassan de forma a subdividi-la em outras duas etapas, de confisco e obtenção – **v. cf. HASSAN, 2019, p. 44-45.**

[153] A doutrina, que lida com o Direito Digital e Informático, traz os devidos tratamentos e cuidados especiais para com o material digital e dispositivos eletrônicos objetos de perícia – **v. cf. ELEUTÉRIO; MACHADO, 2019, p.41-42.**

[154] Discorre sobre os cuidados especiais para o armazenamento de dados em mídia digital – **v. cf. ELEUTÉRIO; MACHADO, 2019, p. 54.**

[155] O raciocínio a ser demonstrado por Sydow, do que vem a ser definido como material pertinente à ser periciado, no tocante aos dados digitais, é ponto de inflexão, mas afirma ser a LGPD instrumento capaz de proteger os dados pessoais dos indivíduos – **v. cf. SYDOW, 2022, p. 142** – pensamento é compatível com os ramos do Direito Processual Penal, quando discute-se a "ponderação" da atividade investigativa – **v. cf. LIMA, 2021, p. 703** –, nada mais lógico que usar raciocínio semelhante na perícia forense digital.

[156] Pensamentos sobre a importância do código hash demonstrado pela doutrina – **v. cf. SYDOW, 2022, p. 207. – Hassan, 2019, p. 62-63. – Eleutério e Machado, 2019, p. 128-129.**

[157] Necessidade de "cópias fiéis" do material digital ao longo da instrução criminal – **v. cf. ELEUTÉRIO; MACHADO, 2019, p. 54** – bem como sua finalidade para comparativos entre as demais funções hash extraídas – **v. cf. SYDOW, 2022, p. 207**.

[158] A análise do material digital extraído, o qual gerou um código hash, deverá ser analisada seguindo os estritos liames com as normas e orientações da perícia forense digital, de modo a analisar "os algoritmos de hash" tanto de entrada quanto de saída **– v. cf. HASSAN, 2019, p. 62 –** pensamento corroborado pela doutrina do Direito Digital e Informático **– v. cf. SYDOW, 2022, p. 207.**

[159] A Tecnologia da Informação traz os elementos essenciais que devem estar contidos em um relatório de perícia digital **– v. cf. HASSAN, 2019, p. 46-47, p. 293**.

[160] O descarte de das provas digitais deve respeitar todas as disciplinas trazidas para as demais provas convencionais, de modo que esta adaptação deve trazer percalços à atividade estatal, mas deve ser empenhada – **v. cf. SOUZA, 2020, p. 197.**

[161] Hassan traz as especificidades da etapa de extração dos dados digitais, levando em conta suas peculiaridades e tendo em perspectiva a existência ou não de técnicas de criptografia capazes de realizar a extração do material de forma a não corrompê-los, tendo ainda as características dos dados contidos em discos rígidos, bem como também os dados contidos em meio de nuvem – **v. cf. HASSAN, 2019, p. 141-142.**

[162] As chamadas técnicas antiforenses são empregadas se valendo também de técnicas de criptografia, de modo a causar uma etapa extra de entrave à atividade investigativa, Hassan as conceitua e as classifica – **v. cf. HASSA, 2019, p. 263.**

[163] Compreensão anteriormente demonstrada sobre o método de cálculo de determinada informação, para obtenção da função unidirecional hash – **v. cf. HASSAN, 2019, p. 62-63.**

A importância da cópia do arquivo original é no intuito de que sejam realizadas as análises do material extraído no documento copiado, viabilizando que o documento original se mantenha integro no dispositivo apreendido, com código hash também já extraído, trazendo assim a possibilidade de realização de uma contraprova pericial, no sentido de comparar os códigos hash extraídos, o da cópia e do original, e demonstrar onde foram feitas alterações realizadas pela perícia investigativa, com qual finalidade foram feitas estas alterações, qual servidor periciou, em qual momento periciou, com que fim, qual atividade determinado perito empenhou, até onde o tratamento de dados dele atingiu, a partir de qual momento novo perito realizou outra alteração, até onde ele foi, novamente com qual intuito, e por assim adiante.

Esta compreensão, acerca do caminho percorrido pelo perito forense digital traz a devida instrumentalização da cadeia de custódia digital em sua melhor forma, isto porque se realiza um passo à passo cronológico, o qual pode ser estabelecido e acompanhado com a devida comparação dos códigos extraídos um diante do outro, seguindo código à código gerado do momento da extração de cada dado digital, sempre se com a premissa de ter a cópia íntegra e o material originário como resguardo e comparativo dos materiais extraídos na perícia, validando assim sua autenticidade e integridade de material, bem como o objeto e o fim destinado pela perícia utilizada em cada uma de suas etapas.

Ou seja, tem-se o material originário com código de extração A, tem-se a cópia pericial íntegra com código de extração B, objeto da perícia, que traz sua cadeia de custódia devido ao acompanhamento de cada alteração realizada adequadamente no curso da investigação, seguindo a cronologia dos códigos extraídos C, D, E, F..., e alterados pelas técnicas periciais adequadas, e tem-se o material alterado incorretamente com extração de códigos B1, C1, D1, E1..., os quais não se realizou o devido procedimento do momento da instrumentalização, sendo assim incomparáveis aos materiais cronológicos de B íntegro, e não servindo assim como meio de obtenção de prova ou como prova em seu fim, diante da sua violação clara à cadeia de custódia digital investigativa.

Caso ocorra alguma violação à qualquer uma destas etapas, ou seja impossível realizar um alinhamento cronológico entre os diversos códigos de extração utilizados ao longo da perícia, deve ser feita a instauração de um procedimento contrapericial, o qual pode ser acionado e provocado pelo investigado ou instaurado de ofício pela autoridade investigativa, para realizar a identificação do momento onde ocorreu a ruptura do devido procedimento quando da instrumentalização, para constatar a inviabilidade da prova. Cabe destacar que tal procedimento se atenta até mesmo para de resguardo para com as ações de responsabilização e

individualização das condutas por parte do investigador que contaminou o material, ou facilitou tal conduta.

Este pensamento acerca da necessidade de se realizar as atividades periciais na cópia se deriva da compreensão de Eleutério e Machado, nota-se:

> [...]
> Devido à fragilidade e sensibilidade das mídias de armazenamento computacional, os exames forenses devem, sempre que possível, ser realizados em cópias fiéis obtidas a partir do material original. (ELEUTÉRIO; MACHADO, 2019, p. 54).
> [...]

Sydow também traz esta importância ao dizer que "*A cópia (clone) é feita em absoluta inteireza para um dispositivo limpo, neutro e não contaminado informaticamente e faz as exatas mesmas vezes do material original*.[164]

Conforme Hassan, os elementos inerentes à um relatório pericial forense digital são: *Informações do investigador; Descrição do caso; Investigação; Resumo das descobertas; Explicação dos termos;* e adverte sobre a necessidade de constar no relatório final do laudo a versão do *software* usado durante o exame pericial. [165] Todas estas informações, conforme descritas acima devem constar do laudo pericial forense digital realizado na investigação criminal.

Estas circunstâncias apresentadas para a devida instrumentalização da informação contida em mídia digital são válidas para quaisquer dados ou metadados digitais, quaisquer informações contidas nestes meios, quaisquer indícios, evidências ou provas ali contidos. Mas algumas peculiaridades se apresentam nos casos de aparelhos telefônicos celulares, bem como os dados contidos em nuvem.

Tal fato se da no caso dos dispositivos celulares pois por se tratarem de um disco rígido portátil, e que em certas ocasiões não são viáveis as realizações de cópias dos dados do dispositivo, devendo assim o próprio dispositivo ser periciado, mas nestes casos Eleutério e Machado[166] ressaltam a importância de um cuidado ainda mais cauteloso por parte do perito que irá realizar o exame do aparelho telefônico e dos dados nele contidos. Mas ainda resta uma incerteza com relação à inexistência de uma cópia fiel do dispositivo original e dos dados nele contidos, devido a possibilidade de alteração dos dados digitais ali inseridos por parte do perito no curso do manuseio do material periciado.

---

[164] **v. cf. SYDOW, 2022, p. 207.**
[165] Destaque realizado no sentido de garantir a integridade da perícia realizada, bem como dos meios empregados nela terem sido os melhores possíveis – **v. cf. HASSAN, 2019, p. 293.**
[166] **v. cf. Eleutério; Machado, 2019, p. 94-95.**

Já com relação aos dados digitais contidos em nuvem, tem-se inerente às próprias características destes o somatório de todos os caracteres dos dados digitais convencionais, acrescidas ainda das características de mundialização[167], virtualização[168], não territorialidade[169], manipulabilidade[170].

Tanto pelo aspecto da perícia forense digital, quanto pelo aspecto da instrumentalização pelos operadores do direito, trazem as mesmas considerações. O pensamento de Hassan se corrobora em Sydow, quando traz a característica de virtualização *como uma natureza dinâmica com uma ampla distribuição de seus componentes por diferentes áreas geográficas*[171]. O inverso também ocorre, Sydow também é corroborado por Hassan com o confronto da não territorialidade ao afirmar que "*todos os critérios da cadeia de custódia informática devem ser seguidos, visto que a não territorialidade exige outros padrões de manutenção e preservação dos indícios.*" [172].

Todas estas peculiaridades devem ser levadas em conta no momento da realização de qualquer atividade estatal que cause reprimenda à um indivíduo que tenha se valido de determinado meio digital para o cometimento de um ilícito penal, ou até mesmo ter se valido deste somente como meio de resguardo de determinada informação contida em mídia digital, que pode vir a ser usada como uma prova digital no curso da investigação criminal conduzida.

Estas são as considerações que devem ser analisadas desde o momento da condução de uma investigação preliminar, indo aos casos de uso destas informações em juízo, no curso de uma ação penal, chegando por fim até mesmo no descarte e eliminação de determinada informação ou dado digital ao final da instrução, devendo resguardar a sua integridade em todas estas etapas.

4.5 Cenário problemático ao contexto apresentado.

Anomia legislativa ou necessidade de adaptação à legislação vigente? Existe a necessidade de adaptação e melhor aplicação dos comandos normativos já existentes através de novas técnicas, métodos e procedimentos mais adequados? Existe a necessidade de edição e promulgação de novas legislações mais atuais e mais condizentes com a realidade factual

[167] Característica trazida pelos ramos do Direito Digital e Informático – **v. cf. SYDOW, 2022, p. 289.**
[168] Também chamada de conectividade – **v. cf. Op. Cit. p. 287.**
[169] **Op. Cit. p. 308.**
[170] **Op. Cit. p. 309.**
[171] **HASSAN, 2019, p. 142.**
[172] **SYDOW, 2022, p. 308.**

existente? Qual solução se apresenta melhor? Quais as diferentes perspectivas sobre o tema? Quais são as correntes doutrinárias que abordaram o tema mais afundo? Quais as implicações de cada uma destas abordagens? Qual destas abordagens se encaixa e se enquadraria melhor com as nossas realidades contemporâneas contidas na nossa sociedade? Existem modelos comparativos a serem utilizados para embasar e fundamentar uma melhor opção de solução das problemáticas e questões existentes? Qual resultado destes modelos comparativos e como eles poderiam ser utilizados frente às realidades da nossa sociedade, tendo em vista as características e cultura que se tem em nosso país? Existe alguma viabilidade de aplicação dos conceitos e normas já existentes ao contexto evolutivo factual que vêm se consolidando? Quais as problemáticas inerentes à aplicação destes conceitos e normas já existentes às problemáticas já existentes e em surgimento? Como deverá ocorrer a regulação das relações em surgimento frente às soluções apresentadas sejam elas quais forem (edição de novas normas ou adaptação às realidades atuais)?

Todas estas questões levantadas devem ser esmiuçadas ao longo dos futuros debates acadêmicos, bem como de toda a comunidade jurídica, até que se encontrem soluções compatíveis com o enfrentamento destas e das demais que vierem a surgir no decorrer dos avanços nestes debates; nesta perspectiva se faz necessário analisar, ao menos parcialmente, essas que foram trazidas.

As primeiras considerações a serem levantadas sobre as problemáticas inerentes ao tema da validade do uso das provas digitais em nuvem no processo criminal é a questão da evolução histórica da utilização das provas digitais. Deve-se lembrar que o direito brasileiro é sabidamente sobrecarregado pelo número de demandas judiciais em curso, bem como de uma atividade legislativa ociosa que não acompanha o ritmo das mudanças sociais contidas no mundo dos fatos, o que por si só ocasiona uma discrepância tremenda entre o cenário factual e o cenário teórico que seria inicialmente analisada determinada situação.

Novos meios de tecnologia vêm sendo desenvolvidos, a todos os momentos, em todos os locais do globo, independente da adaptação ou não dos entes estatais para com estas mudanças; tal situação acaba por gerar, em muitos casos, malferimento à direitos e garantias individuais que acabam por serem sobrepostas ao chamado "*interesse público e da coletividade*".[173]

Para que a atividade estatal, no exercício dos seus poderes, não passe a ser totalmente desregrada, nem tampouco ineficiente, alguns operadores da atividade jurisdicional acabam por pensar em modelos e soluções viáveis às mudanças que constantemente vêm ocorrendo.

[173] Neste ponto se fazem pertinentes as críticas levantadas por parte do movimento doutrinário, que lida com o Direito Processual Penal, de modo que deve existir um "juízo de ponderação" entre a colisão de direitos fundamentais – **v. cf. LIMA, 2021, p. 703.**

Trazendo um concatenamento lógico entre as fragilidades apresentadas, bem como as críticas necessárias à característica inerente dos próprios dados e metadados digitais, deve ser ressaltada também a necessidade de debate frente às autoridades competentes para legislar sobre a matéria e frente aos representantes dos órgãos do poder público que detém poder decisório, tendo em vista as situações às quais se submetem os operadores da norma e do aparato estatal para com o uso destes dados digitais.

Juntamente com estes pontos levantados, devem ser debatidas também as fragilidades da norma vigente, do aparato estatal atualmente utilizado nos Processos Penais e demais procedimentos que utilizam destes dados digitais, das capacidades técnicas dos nossos operadores para com esta realidade, bem como a demonstração dos efetivos riscos ligados aos pontos inerentes às características do uso dos dados, trazendo argumentos relevantes ao debate por todos os entes que tenham competência para auxiliar o poder público e aos indivíduos.

Além de todo o debate no tocante aos aspectos "técnico-digitais" que envolvem o tema, devem-se trazer à baila os aspectos material penal e processual penal, inerentes às características dos dados, ao uso destes e da aplicação legislativa na esfera penal, devendo ser debatidos e demonstrados também os questionamentos que devem ser ressaltados para atingir compatibilidade, ao se buscar uma adaptação, quanto aos raciocínios levantados e ao cabimento destes para o ramo do Direito Penal. Thamay e Tamer (2022, p. 39) explicam que "*[...]A infinidade de situações presentes na sociedade contemporânea parece, por si só, justificar a utilidade da prova digital"*[174].

Após toda esta discussão, haverá uma óbvia necessidade de adaptação para o debate, e posterior implementação eficaz, devendo ser trazidas as diferentes posições e raciocínios, necessários aos novos meios de pensar quanto à problemática e como solucioná-la.

4.5.1 As alterações legislativas na Lei Geral de Proteção de Dados-LGPD e o trato dos dados digitais, bem como a criação da LGPD Penal.

Vale fazer um adendo quanto à necessidade de abordar um dos pontos mais sensíveis aos olhos da discussão temática, que é justamente a problemática que se entrelaça nas questões de liberdades individuais em contrapartida com as prerrogativas excessivas e os limites mínimos do Poder do Estado, que se mostra no cenário fático com cada vez mais frequência. É

[174] **TAMER; THAMAY, 2022, p. 39.**

necessário fazer uma análise acerca das diferentes possibilidades fáticas que podem surgir, inclusive com algumas delas já ocorrendo.

Em primeiro lugar, é sabido que o ente estatal se vale de força e de poderes excessivos, o que acaba ocasionando uma atividade regulatória das relações sociais de forma ostensiva, ainda mais tendo o cenário normativo brasileiro ser demasiadamente analítico, o que se desencadeia em uma série de consequências tanto para o Estado quanto para a sociedade, indo desde encargos excessivos ao ente estatal e chegando até mesmo em ineficiência desta atividade deficitária e ineficácia de certos conjuntos normativos.

Em segundo lugar, é também sabido que as liberdades individuais são direitos cujas garantias legais são vastas, inclusive constitucionais, sendo então base de todos os direitos fundamentais que envolvem o âmbito pessoal de cada indivíduo da sociedade brasileira, devendo ser observadas e respeitadas pelos que irão realizar o exercício do poder estatal, o que acaba por encontrar eventuais confrontos com as necessidades dos entes federativos em realizar a sua atividade investigativa.

Desta forma, além de oneração dos poderes estatais, aqui já se falando tanto do Poder Legislativo quanto do Poder Judiciário e do Poder Executivo, tem-se também atuação regulatória ineficiente, que somada a um excesso de prerrogativas, acaba por consolidar no cenário fático algumas situações de invasão às liberdades individuais e desrespeito aos direitos fundamentais de certos grupos sociais, o que por si já demonstra a imperiosidade em se discutir acerca de quais serão as implicações que serão trazidas por estas violações às garantias legais e constitucionais, e de idêntica forma, buscar alternativas que sejam menos lesivas e que satisfaçam ambas as partes, tanto o Estado em sua atuação reguladora quanto a sociedade que deverá manter suas garantias mínimas.

Eis aqui um dilema apresentado, ao passo que a atividade regulatória do Estado e de seus entes federativos se vê dotada de um poder excessivo, mas necessário para a realização de suas funções investigativas, tem-se que a sociedade busca uma preservação cada vez maior dos seus direitos, gerando assim conflitos de interesses pontuais.

Ainda que não seja de interesse do Estado ter o exercício de seu poder limitado para com as garantias e liberdades individuais, é necessário adotar uma posição mais flexível e observar os comandos normativos de modo a aplicá-los com a maior eficácia possível, desde que não cause o malferimento à direitos e garantias fundamentais.

É o caso nítido e claro das infindáveis proposituras de ações de abuso de poder que estão contidas nas corregedorias dos órgãos estatais e federativos; é também a nítida e clara judicialização excessiva de litígios envolvendo atividade ineficaz e ineficiente de órgãos ou

agentes estatais; é a nítida e clara necessidade de adaptação legislativa constante, haja vista as mudanças normativas não alcançarem todas as ocasiões que se têm no mundo dos fatos.

Aqui se faz necessário abrir a discussão quanto este último ponto da necessidade de adaptação legislativa constante, o que também traz seus problemas, isto porque os agentes do Poder Legislativo jamais conseguirão atingir um nível de atuação de modo a criar comandos normativos que sejam capazes de ter plenitude de abrangência das situações fáticas, mas também estes agentes se valem de muitas atividades regulatórias com conteúdo totalmente esvaziado, que se tornou obsoleto, que já não mais condizem com os costumes e necessidades sociais ou que perderam o objeto, tudo isso ocasionado pela oneração excessiva do Estado como um todo, e claro, de seus poderes e agentes.

Um claro demonstrativo desta situação de onerosidade excessiva do Poder Legislativo é a existência do Projeto de Lei 1.515/2022[175], que visa dispor sobre a regulamentação de segurança estatal e repressão a atividades antijurídicas e infrações penais, ao qual busca alterar a Lei Geral de Proteção de Dados Pessoais-LGPD[176], que vale ressaltar é uma lei de 2018 (recente) cujo já sofreu duas alterações, sendo estas feitas pela Medida Provisória nº 869[177], de 2018, e pela Lei 13.853[178], de 2019, ambas as alterações realizadas no sentido de trazer maior adequação da legislação já existente.

Ainda se atendo à crítica da atuação legislativa, com principal foco voltado à LGPD neste ponto, a realidade factual se mostra tão carente de mudança e adaptação constante que, como já demonstrado, a referida legislação, que foi promulgada em 2018, já sofreu duas alterações em menos de quatro anos de vigência, e ainda se mostram além do PL 1515/2022 mais 22 projetos de Lei até a data do presente estudo, que buscam alterar a redação da legislação vigente em algum sentido, seja para incluir alguma prerrogativa ali não contida, seja para criar algum conceito ali não abordado muito minuciosamente, seja para atribuir alguma proteção a algum preceito ali não descrito, demonstrando uma evidente imperícia da atividade legislativa ao promulgar seus comandos normativos, buscando assim uma compensação quantitativa de infindáveis promulgações de novas legislações constantemente alteradas ou editadas.

Como se pode notar, a necessidade clara de melhor adaptação legislativa se faz imperiosa à medida que novas situações vão surgindo na sociedade, e quando aqui se faz crítica

---

[175] Projeto de Lei, que visa criar a Lei Geral de Proteção de Dados Penal, no intuito de trazer um melhor tratamento de dados pessoais, no que tange aos aspectos da criminalização de atos ilícitos – v. cf. **Projeto de Lei nº 1515, de 2022.**

[176] Dispositivo normativo que traz o tratamento de dados digitais pessoais, bem como o tratamento acerca do sigilo de dados pessoais sensíveis dos indivíduos – **v. cf. Lei Geral de Proteção de Dados – Lei nº 13.709, de 2018.**

[177] Dispositivo normativo que veio a alterar a LGPD, para criar a Autoridade Nacional de Proteção de Dados, mas que já foi substituída posteriormente (Medida Provisória nº 869, de 2018) – **v. cf. BRASIL, 28 dez. 2018.**

[178] A Lei nº 13.853, de 2019, rouxe as alterações à Medida Provisória nª 869 – **v. cf. BRASIL, 20 dez. 2019.**

e se fala em uma busca de adaptação legislativa não se fala em adaptação quantitativa, mas sim qualitativa!!

É necessário se fazer melhor aplicação dos conceitos e normas já existentes, de modo a buscar uma amplitude do entendimento sobre quais ocasiões e situações àquela determinada norma vai alcançar, evitando assim se fazer alterações constantes no comando ali contido; é de idêntica forma necessário buscar uma atuação legislativa mais técnica, mais minuciosa e mais adequada aos costumes, direitos e deveres que envolvem toda a sociedade brasileira daquele determinado momento, de modo a também buscar alcançar o maior número de condições e possibilidades fáticas viáveis daquela determinada regulação normativa, evitando assim também edições constantes e visando uma norma com maior estabilidade e com uma "qualidade de utilização e aplicação" por parte dos operadores dela.

Neste cenário de eventuais situações de confronto dos direitos e deveres do Estado e direitos e deveres da sociedade, fica evidente que será necessário realizar uma adaptação pelas autoridades, órgãos e agentes estatais que irão realizar o enfrentamento das realidades factuais encontradas ao longo das atividades por eles exercidas, de modo a se visar não só os limites da sua atuação como também o aperfeiçoamento da sua atividade e se tornando mais objetivo, com melhor capacidade técnica e mais eficiente.

4.6 Considerações finais.

Ao longo dos debates, chegaram-se à diversas indagações sobre quais as possibilidades de atuação frente ao cenário atual, bem como das diferentes perspectivas e modos de enxergar as situações-problema, o que acarretará em diferentes entendimentos e interpretações sobre qual deverá ser a linha a ser seguida para melhor adequação quanto aos temas discutidos.

Deste modo, foram abordadas também as diferentes possibilidades de enfrentamento, cada uma em relação à sua problemática inerente; passando-se a esta discussão. Diante do cenário atual de contemporaneidade do tema envolto da utilização das provas digitais, e provas digitais em nuvem, no curso do processo penal, tem-se como análise preliminar que as peculiaridades e minúcias que envolvem os dados e metadados digitais acabam por trazer necessidades por parte dos organismos investigativos para se adaptar às especificidades desses, sob pena de trazer um procedimento viciado, eivado de óbices processuais ou até mesmo nulidades, deixando assim fragilidades no curso dos processos penais.

Em segundo ponto, tem-se que a legislação, bem como a posição doutrinária e jurisprudencial tenta se adaptar à rápida e constante evolução dos mecanismos empregados nos meios digitais para o cometimento de ilícitos, mas em sua defasagem temporal de resposta, ocorrem judicializações excessivas para sanar problemas diversos no curso dos processos, os quais poderiam ser sanados ao longo das demandas originárias, se enfrentada mais detalhadamente a questão para evitar lacunas ou brechas à serem exploradas, ou até mesmo realizando um enriquecimento do debate já nas primeiras instâncias.

Por fim, tem-se que algumas experiências do direito comparado, bem como dispositivos contidos em tratados internacionais, os quais o Brasil faz parte e é signatário[179], com outorga devidamente internalizada, podem auxiliar no preenchimento de lacunas normativas, bem como norte para fixação de políticas internas de adequação do aparato investigativo, seguindo os ditames técnicos estabelecidos pelas respectivas áreas da Tecnologia da Informação, bem como as recomendações dos seus experts ligados às áreas da perícia forense digital.

Quanto as indagações realizadas, no sentido da necessidade de edição de novas legislações que sejam mais coerentes com a realidade factual, ou sobre a necessidade de adaptação das legislações vigentes, pode-se discorrer sobre o histórico legislativo do sistema jurídico brasileiro, que acaba por trazer um cenário de superlotação de comandos normativos existentes, muitas vezes até mesmo conflitantes entre si, o que acaba por gerar uma situação de esgotamento das autoridades competentes para realizar a fiscalização destas atividades reguladas pelo poder público, assim podendo trazer uma situação de esvaziamento dos comandos normativos e de inépcia estatal para com estas possíveis legislações editadas exclusivamente para aquele determinado assunto.

Passando-se assim para os questionamentos posteriores, que trazem a necessidade de eventual adaptação procedimental frente à legislações já existentes e ainda em vigência, bem como de melhor capacitação dos profissionais relacionados aos ramos de atuação do Direito Penal e Direito Processual Penal; o que acaba por se mostrar em alguns momentos um raciocínio razoavelmente lógico a ser seguido, porém que também pode trazer inconsistências muito grandes, isto porque poderão ocorrer muitas situações de violação à direitos e garantias fundamentais dos indivíduos em razão da ineficiência de implementação destas medidas em um processo intermediário, trazendo assim efetiva solução aos problemas somente em situações

[179] Promulga a Convenção de Budapeste sobre Cybercrimes – **v. cf. Decreto Lei nº 11.491, de 2023 – v. cf. BRASIL, 13 abr. 2023.**

de pós-consolidação do novo sistema de profissionais atuantes nos ramos, além é claro de um processo dispendioso para o ente estatal em realizar estas capacitações.

Apesar das correntes doutrinárias que versem sobre o tema não serem demasiadas, nem tampouco as mais aprofundadas, existem, ainda em curso, diversos debates sobre a temática, a fim de aprofundar melhor o tema e buscar assim uma solução mais adequada ao tema, porém a realidade é que os ramos do Direito Penal e do Direito Processual Penal não acompanham o passo das evoluções tecnológicas, gerando assim uma situação de disparate de uma realidade para com a outra; deste modo, mostra-se longe do fim o debate sobre o tema e sobre as demais peculiaridades que nele estão inseridos, e o objetivo é justamente buscar este esgotamento de debates para se atingir uma resposta que alcance, se não todas, a maioria das problemáticas que estão inseridas na discussão.

Existem modelos comparativos a serem utilizados em outras localidades do globo, porém, até mesmo pelos poucos defensores de posições doutrinárias mais consolidadas estas comparações não devem ser realizadas, ainda mais levando em conta o cenário atual da sociedade brasileira e do sistema jurídico-processual contido no nosso ordenamento. Isto porque o contexto fático, bem como a estrutura jurídica e social do nosso ordenamento é distinto dos demais contextos em que se realizou esta implementação com mais solitude, assim sendo, diversos são os entendimentos de que a sociedade e o ordenamento jurídico atual têm de passar por estas mudanças, para que por si só sejam implementadas as alterações no contexto fático adequado ao nosso cenário.

5. CONCLUSÃO

Por fim, se compreender as implicações fáticas trazidas pelo tema e tentar visualizar soluções condizentes e viáveis de implementação, seja através dos mecanismos e aparatos estatais já existentes, seja pela criação de novos instrumentos neste sentido.

Esta é a conclusão inicialmente encontrada, no sentido de fazer melhor aplicação dos mecanismos processuais e procedimentais existentes, bem como melhor capacitação dos recursos humanos disponíveis e utilizados ao longo do processo de utilização dos dados digitais em nuvem no processo criminal; ou, em outras ocasiões, realizar a implementação, edição e promulgação de novos dispositivos normativos, que habilitem os recursos humanos e mecanismos já disponíveis de terem melhor efetividade e eficácia no curso dos processos penais já em andamento.

Algumas das discussões e debates ainda devem ser aprofundados pela comunidade acadêmica e jurídica como um todo, em principal a comunidade atuante nos ramos do Direito Penal e Direito Processual Penal, na busca de aprofundamento dos conhecimentos e perspectivas contidas.

Parte do movimento doutrinário, que está explorando esta temática, traz a situação de anomia legislativa, enquanto outra parte discute apenas uma melhor adaptação estrutural dos aparatos estatais existentes, visando realizar uma compatibilização entre os sistemas legislativos vigentes e as inovações tecnológicas apresentadas. Nota-se em:

> [...]
>
> Da mesma forma, do ponto de vista normativo, tanto os trabalhos de observação, de caráter exploratório, analítico ou empírico, quanto aqueles propositivos partem, por exemplo, de experiências comparadas sobre as formas pelas quais o direito, com suas construções teóricas, doutrinárias e narrativas, enfrenta a natureza polissêmica das tecnologias: órgãos legislativos, executivos e judiciais devem manter diálogos com aspectos técnicos, políticos, econômicos e sociais implicados nos segmentos tecnológicos ao redor do globo, confrontando-os com os distintos países e seus sistemas jurídicos. Isso porque entre as principais características dos bens tecnológicos e informacionais está sua inequívoca mobilidade além-fronteiras. (POLIDO; BRANDÃO; ROSINA, p. 396).
>
> [...]

De maneira que o tema vai sendo melhor estudado e debatido nas rodas acadêmicas, bem como na seara do Poder Judiciário na aplicação de casos concretos, mostram-se melhores avanços quanto à adaptação necessária, e leva assim uma mobilização do aparato estatal como um todo, tornando-se assim capaz de enfrentar adequadamente as peculiaridades trazidas por cada etapa de inovação tecnológica trazida pela sociedade contemporânea e pelo seu uso da tecnologia; é algo cada vez mais rotineiro e se adapta em velocidade muito acelerada, sendo este exatamente o caso dos dados e metadados digitais em nuvem, bem como a IA, os quais demonstram a severa situação que se encontra o cenário normativo global atual, e como fazer frente à essas inovações. É a posição de parte da doutrina que discute inicialmente o tema, veja:

> [...]
>
> Em ciclos cada vez menores e mais acelerados de inovação, a pesquisa jurídica deve romper com seu tradicional isolamento, a fim de compreender as intersecções com diferentes áreas: ciência da computação, economia, administração, antropologia, sociologia, filosofia, ciências políticas e de Estado.(POLIDO; BRANDÃO; ROSINA, p. 397).
>
> [...]

Conclusivamente são demonstradas, de forma lógica e concatenada, as diferentes possibilidades que estão se desdobrando no cenário doutrinário e teórico, sendo essas: a) a anomia legislativa, relacionada à ausência de previsão normativa das situações procedimentais,

vinculadas ao uso de dados e metadados digitais em nuvem como meio de prova nos processos penais; b) adaptação técnica e uma melhor regulamentação quanto à utilização de recursos e estrutura, aqui se tratando de procedimentos técnicos e de material humano capaz de lidar mais adequadamente com o uso dos dados e metadados digitais em nuvem.

Ambas as possibilidades demonstradas são discutidas, no sentido de trazer idênticos posicionamentos lógicos nos ramos da atuação dos poderes legislativo e judiciário, para realizar enfrentamento das questões, de modo que pode ocorrer: a1) a implementação de uma corrente jurisprudencial dominante, que seja capaz de suprir as defasagens entre o avanço da tecnologia e a atuação dos profissionais forenses e jurídicos, de modo a manter uma coerência da atuação estatal para com a observância da norma vigente (de difícil implementação diante das alterações constantes e incompatibilidades doutrinárias adotada pelos magistrados); a2) a edição de nova legislação, que seja capaz de realizar a efetiva adequação, entre os procedimentos necessários para observância da norma editada e os direitos e garantias sociais e individuais, de modo a não trazer uma situação de ineficiência da atuação estatal nem ausência desta, mas que identicamente não gere abusos; ou/e b) realizar uma melhor capacitação de material humano, bem como de melhor investimento na estrutura do aparato estatal responsável pela atividade jurisdicional, de modo a garantir uma melhor qualidade do serviço investigativo, e de modo a realizar uma melhor observância da norma vigente, a qual se encontra ultrapassada, mas visando garantir eficiência estatal e eficácia da atividade jurisdicional.

6. BIBLIOGRAFIA

AFP. Itália bloqueia ChatGPT por não respeitar legislação sobre dados pessoais. 31 mar. 2023. Disponível em: < https://www.cartacapital.com.br/tecnologia/italia-bloqueia-chatgpt-por-nao-respeitar-legislacao-sobre-dados-pessoais/ > e < https://www.em.com.br/app/noticia/internacional/2023/03/31/interna_internacional,1476256/italia-bloqueia-chatgpt-por-nao-respeitar-leis-sobre-dados-pessoais.shtml >. Acessado em: 17 abr. 2024.

ALVAREZ, Vanessa. União Europeia debate pacote de regras para região sobre inteligência artificial. Revista Consultor Jurídico-ConJur. 3 abr. 2023. Disponível em: < https://www.conjur.com.br/2023-abr-03/vanessa-alvarez-chatgpt-mira-autoridades-europeias/ >. Acessado em: 17 abr. 2024.

ARARAKI, Ana; ARARAKI, Filipe. Dados e Metadados - conceitos e relações. Revista Ci.Inf., Brasília, DF, v.49 n.3, p.34- 45, set./dez. 2020. Publicada em 28 jul. 2021. Disponível em: https://revista.ibict.br/ciinf/issue/view/294/71 Acessado em: 7 abr. 2024.

ARAÚJO, Liamari. Estudo de aplicações de técnicas de acesso IP-VPN em laboratórios de informática do ProInfo nas escolas da Grande Florianópolis. Instituto Federal de Santa Catarina-IFSC. 7 maio 2014. Disponível em: < https://wiki.sj.ifsc.edu.br/index.php/Estudo_de_aplica%C3%A7%C3%B5es_de_t%C3%A9cnicas_de_acesso_IP-VPN_em_laborat%C3%B3rios_de_inform%C3%A1tica_do_ProInfo_nas_escolas_da_Grande_Florian%C3%B3polis. > Acessado em: 17 abr. 2024.

AVELAR, Daniel Ribeiro Surdi de; MUNIZ, Gina; SAMPAIO, Denis; SILVA, Rodrigo Faucz Pereira. Sistema de justiça criminal: cadeia de custódia no contexto das provas digitais. Revista Consultor Jurídico-ConJur. 30 mar. 2024. Disponível em: < https://www.conjur.com.br/2024-mar-30/cadeia-de-custodia-da-prova-digital/ >. Acessado em: 17 abr. 2024.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal - parte geral 1. 22. ed. rev. ampl. e atual. São Paulo. Saraiva, 2016.

BRAGA, Lucas; TOLEDO, Victor. VPN: o que é, para que serve e como funciona o acesso em uma rede privada. Tecnoblog. Mar. 2024. Disponível em: < https://tecnoblog.net/responde/vpn-o-que-e-para-que-serve-e-como-funciona-o-acesso-em-uma-rede-privada/ >. Acessado em: 17 abr. 2024.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm

BRASIL. Decreto nº 592, 6 jun. 1992. Atos Internacionais. Pacto Internacional sobre os Direitos Civis e Políticos. Promulgação. Diário Oficial da União: seção 1, Brasília, DF, 7 jul. 1992. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm >

BRASIL. Decreto nº 3.321, 30 dez. 1999. Promulga o Protocolo Adicional à Convenção Americana sobre Direitos Humanos em Matéria de Direitos Econômicos, Sociais e Culturais "Protocolo de São Salvador", concluído em 17 de novembro de 1988, em São Salvador, El Salvador. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto/d3321.htm >

BRASIL. Decreto nº 11.491, 12 abr. 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro

de 2001. Diário Oficial da União: seção 1, Brasília, DF, 13 abr. 2023. Disponível em: < https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001 >

BRASIL. Decreto Legislativo nº 27, de 1992. Aprova o texto da Convenção Americana sobre Direitos Humanos (Pacto São José) celebrado em São José da Costa Rica, em 22 de novembro de 1969, por ocasião da Conferência especializada Interamericana sobre Direitos Humanos. Disponível em: < https://www2.camara.leg.br/legin/fed/decleg/1992/decretolegislativo-27-26-maio-1992-358314-exposicaodemotivos-143572-pl.html > e < https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/anexo/and678-92.pdf >.

BRASIL. Decreto Legislativo nº 37, 17 dez. 2021. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Diário Oficial da União: seção 1, Brasília, DF, 17 dez. 2021. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/12/2021&jornal=515&pagina=7 &totalArquivos=188

BRASIL. Decreto Lei nº 2.848, de 7 dez. 1940. Código Penal. Diário Oficial da União: seção 1, Brasília, DF, 3 abr. 1941. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm >
.
BRASIL. Decreto Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Diário Oficial da União: seção 1, Brasília, DF, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm .

BRASIL. Lei nº 9.504, 30 set. 1997. Estabelece normas para as eleições. Diário Oficial da União: seção 1, Brasília, DF, 1 out. 1997. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l9504.htm >

BRASIL. Lei nº 10.406, 10 jan. 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 11 jan. 2002. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm >

BRASIL. Lei nº 12.965, 23 abr. 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em:
https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados-LGPD. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=15/08/2018&jornal=515&pagina=59

BRASIL. Lei nº 13.853, 8 jul. 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 20 dez. 2019. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

BRASIL. Medida Provisória nº 869, 27 dez. 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 28 dez. 2018. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm >

BRASIL. Medida Provisória nº 2.200-2, 27 ago. 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 27 ago. 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm >

BRASIL. Projeto de Lei nº 1515/2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em: < https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#tramitacoes >. Acessado em: 17 abr. 2024.

BRASIL, Supremo Tribunal Federal (STF). A Constituição e o Supremo. Brasília: Secretaria de Documentação, 2011.

BUDAPESTE. Convenção sobre o Cibercrime. Conselho da Europa, 23 nov. 2001. Disponível em: https://rm.coe.int/16802fa428 e https://www.coe.int/en/web/cybercrime/the-budapest-convention#

BUNDESMINISTERIUM. Bundesdatenschutzgesetz. Disponível em: < https://www.bmi.bund.de/DE/themen/verfassung/datenschutz/bundesdatenschutzgesetz/bundesdatenschutzgesetz-node.html > e < https://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf >. Acessado em 15 mar. 2023.

CAPEZ, Fernando. Sistema acusatório e garantias do Processo Penal. Revista Consultor Jurídico-ConJur. 7 out. 2021. Disponível em: < https://www.conjur.com.br/2021-out-07/controversias-juridicas-sistema-acusatorio-garantias-processo-penal/ >. Acessado em: 1 abr. 2024.

DANIELE, MARCELLO. La prova digitale nel processo penale. Rivista di Diritto Processuale, 2011. Disponível em: < https://www.academia.edu/31481406/La_prova_digitale_nel_processo_penale >. Acessado em: 17 abr. 2024.

DIREITO, Dizer. São inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos. Revista Dizer Direito. 7 mar. 2023. Disponível em: < https://www.dizerodireito.com.br/2023/03/sao-inadmissiveis-as-provas-digitais.html > Acessado em: 17 abr. 2024.

DUARTE, Otto Carlos Muniz Bandeira; MIRANDA, Ivana Cardial. VPN-Virtual Private Networl, Rede Privada Virutal. Grupo de Teleinformática e Automação da Universidade Federal do Rio de Janeiro-GTA/UFRJ. Disponível em: < https://www.gta.ufrj.br/seminarios/semin2002_1/Ivana/ >. Acessado em: 17 abr. 2024.

EUROPE, Council. The Budapest Convention (ETS No. 185) and its Protocols. Disponível em: < https://www.coe.int/en/web/cybercrime/the-budapest-convention >. Acessado em 15 mar. 2023.

EUROPE, Council. Convention nª 108 on data protection - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Disponível em: < https://rm.coe.int/1680078b37 > e < https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108 >. Acessado em: 15 mar. 2023.

EUROPE, Council. Data Protection under GDPR. Disponível em: < https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm >. Acessado em: 15 mar. 2023.

EUROPE, Council. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046 >. Acessado em: 15 mar. 2023.

EUROPE, Council. Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 >. Acessado em: 15 mar. 2023.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Márcio Pereira. Desvendando a computação forense. 7. imp. Novatec Editora Ltda, 2019.

ESPANHA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponível em: < https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673 >. Acessado em: 15 mar. 2023.

ESPIÑERA, Bruno; CAVALOPE, Luís Eduardo; FILHO, Maurício Mattos (org.). A prova e o processo penal constitucionalizado: estudos em homenagem ao ministro Sebastião Reis Júnior. 1. ed. São Paulo. Editora D'Plácido, 2022.

GOMES, Rodolfo Perini. Superação Prospectiva (Prospective Overruling) como regra - (in)segurança jurídica em caso de virada jurisprudencial. Disponível em: < https://revistajuridica.tjdft.jus.br/index.php/rdj/article/download/535/97/2079 >. Acessado em: 17 abr. 2024.

HASSAN, Nihad A. Perícia forense digital: guia prático com uso do sistema operacional Windows. São Paulo. Novatec Editora Ltda, 2019.

ITALIANO, Parlamento. Decreto Legislativo 30 giugno 2003, nº 196, “Codice in Materia di Protezione dei Dati Personali”. Disponível em: < https://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm >. Acessado em: 15 mar. 2023.

LIMA, Renato Brasileiro. Manual de Processo Penal: vol. único. 10 ed. rev. ampl. atual. Ed. Juspodium, São Paulo, 2021.

LONG, Johnny; GARDNER, Bill; BROWN, Justin. Google Hacking para Pentest. 1 ed. São Paulo: Novatec Editora Ltda, 2018.

LOPES JR. Aury. Direito Processual Penal. 20 ed. São Paulo. SaraivaJur, 2023.

LUCCHESI, Guilherme Brenner; ZONTA, Ivan Navarro. Apontamentos sobre a Cadeia de Custódia da Prova Digital no Processo Penal. Instituto Brasileiro de Direito Penal Eletrônico-IBDPE. 23 fev. 2021. Disponível em: < https://ibdpe.com.br/ccpdpp/?_ga=2.229494812.1478074301.1697384427-1456869735.1697384427 >. Acessado em: 17 abr. 2024.

NATIONS, United. Declaração Universal dos Direitos Humanos. Disponível em: < https://brasil.un.org/pt-br/91601-declara%C3%A7%C3%A3o-universal-dos-direitos-humanos > e < https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por > e < https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos >. Acessado em: 15 mar. 2023.

NUCCI, Guilherme de Souza. Código Penal comentado. 20. ed. rev. atual. e ampl. Rio de Janeiro. Forense, 2020.

NUCCI, Guilherme de Souza. Leis Penais e Processuais Penais Comentadas. v. 1. 14. ed. rev. atual. e ref. Rio de Janeiro. Forense, 2021.

NUCCI, Guilherme de Souza. Manual de Direito Penal. 18 ed. rev. atual. e ampl. Rio de Janeiro. Forense. 2022.

NUCCI, Guilherme de Souza. Provas no Processo Penal. 5. ed. rev. atual. e ampl. Rio de Janeiro. Forense, 2022.

OLIVEIRA, Sérgio de Oliveira. Internet das Coisas - com ESP8266, arduino e raspberry pi. 2. ed. São Paulo. Novatech Editora Ltda, 2021.

OLIVEIRA, Vinicius Machado. Identificação, coleta, aquisição e preservação de evidência. Disponível em: <https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/ >Acessado em: 15 out 2023.

PITTIRUTI, Marco. Digital evidence e *procedimento penale*. Torino: Giappichelli, 2017.

POLIDO, Fabrício; BRANDÃO, Luiza; ROSINA, Mônica Steffen Guise. Direito e Tecnologia. *in:* Metodologia da pesquisa em direito : técnicas e abordagens para elaboração de monografias, dissertações e teses / coordenadores: Marina Feferbaum, Rafael Mafei Rabelo Queiroz. – 2. ed. – São Paulo : Saraiva, 2019.

POLITIZE. Revista Polítize. O Sistema Internacional de Proteção e os tratados internacionais de Direitos Humanos. Disponível em: < https://www.politize.com.br/equidade/tratados-internacionais-de-direitos-humanos/ >. Acessado em: 17 abr. 2024.

PROKISCH, Carlos A. Cibersegurança: como proteger seus dados no mundo digital. São Paulo. Editora SENAC São Paulo, 2023.

SANTOS, Bruna Martins. Convenção de Budapeste sobre o Cibercrime na América Latina – uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México. Derechos Digitales. Maio 2022. Disponível em: < https://www.derechosdigitales.org/wp-content/uploads/PT-Ciberdelincuencia-2022.pdf >. Acessado em: 15 mar. 2023.

SILVA, Naiara Lisboa da. O Princípio da Paridade de Armas como uma ficção jurídica no Processo Penal Brasileiro – uma análise sobre a violação do princípio e suas consequências. Disponível em: < https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2018/pdf/NaiaraLisboadaSilva.pdf > Acessado em: 17 abr. 2024.

SIMÃO, Bárbara; CRUZ, Francisco Brito. [editores]. Direitos fundamentais e processo penal na era digital - doutrina e prática em debate. v. 5. São Paulo: InternetLab, 2022.

SOUZA, Sérgio Ricardo de. Prova penal e tecnologia: novas técnicas e meios de investigação e captação de provas. Curitiba. Juruá, 2020.

STALLINGS, William. Arquitetura e organização de computadores / William Stallings; com contribuição de Peter Zeno; com prefácio de Chris Jesshope ; tradução Sérgio Nascimento ; revisão técnica Ricardo Pannain. - 10. ed. - São Paulo: Pearson Education do Brasil, 2017.

STJ. A cadeia de custódia no processo penal: do Pacote Anticrime à jurisprudência do STJ. Secretaria de Comunicação Social do Superior Tribunal de Justiça. 23 abr. 2023. Disponível em: < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/23042023-A-cadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia-do-STJ.aspx >. Acessado em: 17 abr. 2024.

STJ. Decisão Monocrática. HC 879.276/SP, rel. Min. Antônio Saldanha Palheiro, julgado em 19 dez. 2023, publicado *in* DJ-e em 21 dez. 2023.

STJ. Quinta Turma. RHC 77.836/PA, rel. Min. Ribeiro Dantas, julgado em 5 fev. 2019, publicado *in* DJ-e em 12 fev. 2019.

STJ, Quinta Turma, AgRg no RHC 143.169/RJ, rel. Min. Messod Azulay, rel. acórdão Min. Ribeiro Dantas, julgado em 7 fev. 2023, publicado in DJ-e em 1 mar. 2023.

STJ, Sexta Turma. RHC 99.735/SC, rel. Min. Laurita Vaz, julgado em 27 nov.2018, publicado in DJ-e em 12 dez.2018.

STJ, Sexta Turma. AgRg no RHC 133.430/PE, rel. Min. Nefi Cordeiro, julgado em 23 fev. 2021, publicado in DJ-e em 26 fev. 2021.

STJ, Sexta Turma. AgRG no HC 735.027/SP, rel. Min. Sebastião Reis Júnior, julgado em 26 set. 2023, publicado in DJ-e em 4 out.2023.

SYDOW, Spencer Toth. Curso de Direito Penal Informático. 3. ed. rev. e atual. Salvador. Editora JusPodivm, 2022.

THAMAY, Rennan; TAMER, Maurício. Provas no Direito Digital - Conceito da prova digital, procedimentos e provas digitais em espécie. 2. ed. São Paulo. Revista dos Tribunais, 2022.

TRF1. Tribunal Regional Federal da Primeira Região. HC 1033633-48.2022.4.01.0000, rel. Des. Fed. Ney Belo, julgado em 13 out. 2022, publicado in DJ-e em 13 out. 2022.

TRF3. Tribunal Regional Federal da Terceira Região. Ciência da Informaçãov. 49 n.3 set./dez. 2020 – Edição Especial Temática – Ciência de dados na ciência da informação. TRF3. Editada abr. 2021. Publicada jul. 2021. Disponível em: < https://revista.ibict.br/ciinf/issue/view/294 >. Acessado em: 7 abr. 2024.

VITAL, Danilo. Nulidade por quebra da cadeia de custódia deve ser sopesada pelo juiz, diz STJ. Revista Consultor Jurídico-ConJur. 27 nov. 2021. Disponível em: < https://www.conjur.com.br/2021-nov-27/nulidade-quebra-cadeia-custodia-sopesada-juiz/ >. Acessado em: 17 abr. 2024.

VITAL, Danilo. STJ reconhece quebra da cadeia de custódia e anula provas digitais. Revista Consultor Jurídico-ConJur. 6 mar. 2023. Disponível em: < https://www.conjur.com.br/2023-mar-06/stj-reconhece-quebra-cadeia-custodia-anula-provas-digitais/ >. Acessado em: 17 abr. 2024.

WEBER, Jonathan. Google Analytics e a Google Tag Manager para desenvolvedores. 1. ed. Novatec Editora Ltda, 2016.

WEIDMAN, Georgia. Testes de invasão – uma introdução prática ao hacking. 9ª reimp. São Paulo. Novatec, 2022.

ZAREMBA. Opera e VPN SurfEasy: O combo para privacidade online. Blogs Opera, 2015. Disponível em: < https://blogs.opera.com/brazil/2015/09/opera-e-vpn-surfeasy-o-combo-para-privacidade-online/>. Acesso em 15. Ago. 2023.