Universidade de Brasília – UnB

Faculdade de Direito

LUCIEN ROCHA LUCIEN

ACREDITAÇÃO E ADMISSIBILIDADE DE EVIDÊNCIAS DIGITAIS DE CRIMES CIBERNÉTICOS PRATICADOS EM COMPUTAÇÃO DE NUVEM:

DESAFIOS NA ESFERA JUDICIAL DO BRASIL

BRASÍLIA – DF

2023

Lucien Rocha Lucien

ACREDITAÇÃO E ADMISSIBILIDADE DE EVIDÊNCIAS DIGITAIS DE CRIMES CIBERNÉTICOS PRATICADOS EM COMPUTAÇÃO DE NUVEM:

DESAFIOS NA ESFERA JUDICIAL DO BRASIL

Dissertação apresentada à Faculdade de Direito da Universidade de Brasília como requisito parcial à obtenção do grau de Mestre, no Programa de Mestrado Profissional em Direito, Regulação e Políticas Públicas.

Orientador: Prof. Dr. João Costa-Neto

Brasília
2023

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Lucien, Lucien Rocha
LL937a ACREDITAÇÃO E ADMISSIBILIDADE DE EVIDÊNCIAS DIGITAIS DE CRIMES CIBERNÉTICOS PRATICADOS EM COMPUTAÇÃO DE NUVEM: DESAFIOS NA ESFERA JUDICIAL DO BRASIL / Lucien Rocha Lucien; orientador Joao Costa-Neto. -- Brasília, 2023.
124 p.

Dissertação(Mestrado em Direito) -- Universidade de Brasília, 2023.

1. Cibercrime. 2. Computação em nuvem. 3. Evidência digital. 4. Regulação. 5. Direito Comparado. I. Costa-Neto, Joao, orient. II. Título.

FOLHA DE APROVAÇÃO

Dissertação intitulada “**Acreditação e admissibilidade de evidências digitais de crimes cibernéticos praticados em computação de nuvem: desafios na esfera judicial do brasil**”, apresentada à banca avaliadora em 22 de novembro de 2023.

BANCA EXAMINADORA

Prof. Dr. João Costa-Neto
(Orientador – Presidente)

Prof. Dr. José Querino Tavares Neto
(Membro Externo)

Prof. Dr. Benedito Cerezzo Pereira Filho
(Membro)

Prof. Dra. Fernanda de Carvalho
(Membro)

Profa. Dra Eneá de Stutz e Almeida
(Membro Suplente)

Aprovada em: 22 de novembro de 2023.

À minha esposa Edilene, pelo apoio incondicional e constante incentivo ao meu desenvolvimento acadêmico.

Ao meu filho Lucian, pela compreensão e paciência pelas horas dedicadas para a concepção desta pesquisa.

AGRADECIMENTOS

- A meus pais, Mário e Eliene (*in memoriam*), pelos valores transmitidos e pelas oportunidades proporcionadas;
- Aos Gestores da Escola Judicial do Amapá (EJAP), Tribunal de Justiça do Estado do Amapá (TJAP) e Instituto Federal do Amapá (IFAP), que juntamente com a Professora Dra. Eneá Stutz e Almeida/UNB foram incansáveis na concretização do Mestrado Interinstitucional (MINTER) junto à UNB;
- Ao Professor Dr. João Costa-Neto, por aceitar a orientação desta pesquisa e conduzir seu desenvolvimento com dedicação;
- Aos professores membros da banca avaliadora, pelas valiosas contribuições no aperfeiçoamento do trabalho;
- A Irene e Luciana pelas preciosas sugestões de revisão e melhorias deste trabalho;
- A colega de turma Lêda Lima e Aline Portela (UnB) pelos inestimáveis conselhos e contribuições;
- A todos, que de alguma forma, contribuíram para a concretização desta importante etapa em minha carreira acadêmica.

RESUMO

A evolução da Tecnologia da Informação tem alcançado níveis até então inimagináveis, a exemplo do desenvolvimento da computação em nuvem, considerada uma “virtualização dos *data centers*”. Essa evolução se apresenta concretamente nos serviços disponibilizados à sociedade e que a tornaram, em certa medida, dependente da tecnologia para otimizar suas rotinas e desenvolver novas relações sociais e até de negócios. No entanto, paralelamente a esses benefícios, o contingente de dados digitais envolvidos nas relações viabilizadas pela estrutura da Internet possibilita o desenvolvimento de ações ilícitas, fomentando cibercrimes, que acompanham a evolução tecnológica *pari passu* em tempo e em sofisticação, como é o caso dos crimes praticados com a computação em nuvem. O contexto desse tipo de computação envolve uma distribuição geográfica mundial de dados de difícil acesso, implementada segundo interesses particulares das *Big Techs*. Esse é o escopo deste trabalho, que tem como objetivo avaliar o instituto da regulação na esfera administrativa (autorregulação regulada), como meio de assegurar padrões de confiabilidade à cadeia de custódia de evidências digitais obtidas em ambientes de nuvem computacional. Em última instância, visa-se à admissibilidade de evidências digitais como prova em cibercrimes. O estudo demonstra o *status* do ordenamento brasileiro em relação ao combate ao cibercrime e no Direito Comparado. Metodologicamente, a pesquisa é classificada como bibliográfica e concluiu-se pela possibilidade de se regular, de forma autorregulada, os critérios para a cadeia de custódia das evidências digitais de cibercrimes praticados no ambiente da computação em nuvem.

Palavras-chaves: Cibercrime. Computação em nuvem. Evidência digital. Regulação. Direito Comparado.

ABSTRACT

The evolution of Information Technology has reached previously unimaginable levels, such as the development of cloud computing, considered a "virtualization of data centers". This evolution can be seen concretely in the services made available to society, which have made it, to a certain extent, dependent on technology to optimize its routines and develop new social and business relationships. However, alongside these benefits, the amount of digital data made possible by the structure of the Internet enables the development of illicit actions, fostering cybercrime, which accompanies technological evolution both in time and sophistication, as is the case with crimes committed using cloud computing. The context of this type of computing involves a worldwide geographical distribution of data that is difficult to access, implemented according to the particular interests of Big Tech. Within this context, this study aims to evaluate regulation in the administrative sphere (regulated self-regulation), as a means of ensuring standards of reliability in the chain of custody of digital evidence obtained in cloud computing environments. Ultimately, the goal is to examine the admissibility of digital evidence as proof in cybercrime cases. The study demonstrates the current status of the Brazilian legal system in combating cybercrime in comparison to other legal systems. In terms of methodology, the study is classified as bibliographical and concludes that it is possible to self-regulate the criteria for the chain of custody of digital evidence of cybercrimes committed in a cloud computing environment.

Keywords: Cybercrime. Cloud computing. Digital evidence. Regulation. Comparative law.

LISTA DE QUADROS E FIGURAS

SUMÁRIO

INTRODUÇÃO

Na velocidade com que as informações vêm sendo repassadas e com os reflexos que isso impõe às relações em sociedade e, consequentemente, a tudo o que delas decorre, a expressão “modernidade líquida” parece abarcar e resumir bem as características do tempo presente. O sociólogo Zygmunt Bauman (2007, apud ALMAS; GASTAL, 2021, p. 4), autor dessa expressão, explica: “Os tempos são ‘líquidos’ porque tudo muda rapidamente. Nada é feito para durar, para ser ‘sólido’”.

Mas a ideia de que “nada é feito para durar” tem implicações no curso das relações em sociedade, na medida em que essas, em sua instantaneidade, esbarram em crimes cometidos contra os direitos fundamentais, aspectos duráveis cuja tutela requer cuidados e atenções detalhados. E se isso, por um lado, exige uma certa celeridade por parte do Direito, para continuar assegurando a referida tutela, por outro, a velocidade das informações, que abrange todas as áreas da vida, por sua própria forma de desenvolvimento, desencadeou outra realidade, paralelamente à realidade habitual concreta: a virtual.

São tantas as inovações e tecnologias que seu uso se impõe no cotidiano, sendo muitas vezes difícil diferenciar a vida real da vida virtual: uma acaba por se tornar uma extensão da outra. E o Direito precisa se atualizar para conseguir manter a ordem social e para tutelar a liberdade e os direitos fundamentais dos indivíduos no ciberespaço, permitindo sua participação democrática nele e fora dele.

A seu turno, o Direito vem procurando “chegar” às atividades regidas pela tecnologia, à medida que as ocorrências vão aparecendo e as tutelas vão sendo reclamadas. É assim que tem acontecido de certa forma, até porque, no caso dos avanços tecnológicos, não há como se estabelecer outra garantia para um direito reconhecido e já devidamente tutelado. A questão é que esse direito foi agredido ou não foi respeitado por alguém de identidade ignorada e cujo crime não tem lugar identificado nem provas palpáveis. Trata-se do modo e do meio utilizados para contornar esse direito. Há aí um componente qualitativo com o qual o Direito tem de lidar.

Em outro ponto, da mesma forma que a tecnologia está cada vez mais presente no cotidiano da sociedade, os crimes têm se utilizado do ambiente tecnológico no mesmo patamar de intensidade e de presença e ainda com alto nível de sofisticação. O componente aí é quantitativo, qualitativo e recorrente.

A tecnologia atua em um ciberespaço, ambiente digital constituído de rede de computadores, a Internet, levando a questionamentos sobre “quem e onde” em relação aos crimes. Já as ações investigativas, com base no Direito, necessitam de dados concretos, objetivos, como reconhecimento de pessoas e provas – isso apenas para ilustrar a comparação. Há uma cadeia de custódia que não pode ser quebrada. O Direito tem os elementos substanciais do crime, mas na prática faltam os meios adequados para agir nesse novo ambiente. Assim, há direitos tutelados, mas faltam meios para combater os crimes contra eles de forma pontual.

E é nesse sentido que vêm sendo envidados esforços e desenvolvidas outras vertentes de estudo, como Direito do Ciberespaço, por exemplo, debatido nos Estados Unidos desde os anos 1980 e constituído de leis, regulamentações e conjunto de práticas contratuais de vários tipos, envolvendo usos e funcionamentos de computadores e de *softwares*. A finalidade é a criação de regras para comunicações e negócios em rede (CERQUEIRA, 1999, p. 2).

Todavia, paralelamente aos novos estudos sobre como solucionar os cibercrimes, é unânime o entendimento de que combatê-los demanda o uso de metodologias sempre atualizadas e de ponderações técnicas na condução de processos investigativos pelas autoridades policiais, sob pena de se inviabilizar a aquisição e/ou coleta de evidências pelos órgãos de aplicação de leis ou sua admissibilidade como prova. Em consequência, dificulta-se a punição.

Nessa perspectiva, no que diz respeito ao controle de crimes no ambiente tecnológico, o atual cenário jurídico brasileiro ainda se encontra defasado por razões observadas em distintas perspectivas: seja pela própria dificuldade de acompanhar a evolução da tecnologia e os concomitantes crimes cibernéticos; seja pelas variantes sempre inovadoras desses crimes; seja em razão do processo burocrático da função legiferante ou talvez pelo conjunto dessas causas.

A realidade é que, mesmo com as inovações trazidas ao Código de Processo Penal pela Lei n. 13.964/2019 – que “aperfeiçoa a legislação penal e processual penal” –, a legislação brasileira apenas disciplina a necessidade de preservação da cadeia de custódia em sentido amplo. Ela limita sua aplicação à custódia de artefatos físicos, não enfrentando particularidades, por exemplo, as características das provas digitais, como volatilidade do elemento eletrônico e cadeia de acesso digital.

A par disso, apesar dos esforços envidados na criação de leis específicas que tipificam o crime digital na esfera brasileira, dos acordos de assistência jurídica em matéria penal – a exemplo das Leis n. 13.964/2019 (que atualiza o Código de Processo Penal com o pacote anticrime) e n. 12.965/2014 (que disciplina uso da Internet) – e da recente adesão do Brasil ao tratado sobre crime cibernético – a Convenção sobre o Cibercrime ou Convenção de Budapeste –, a discrepância entre a velocidade de evolução e de uso das tecnologias digitais e a complexidade de aprovação de instrumentos legais é fator de peso e impossibilita que a legislação determine procedimentos e processos específicos para cada tipo de tecnologia, sob pena de a nova lei já nascer desatualizada.

No plano da prática cotidiana, ainda se destacam as limitações atuais dos sistemas do processo eletrônico judicial brasileiro, que restringem o quantitativo de espaço disponível para a juntada de arquivos nos processos judiciais. Com isso, inviabiliza-se ou força-se a aceitabilidade de dispositivo físico (HD, DVD, Blu-Ray, etc.) como prova juntada ao processo por meio do uso de instrumentos como a certidão e a ata notarial, bem como o uso de recursos como Quick Response Code (QR Code), código de resposta rápida (código de barras bidimensional), Uniform Resource Locator (URLs) ou endereços web, para fazer constar nos autos provas armazenadas em outros repositórios fora do controle dos sistemas de informações do judiciário.

Thamay e Tamer (2022, p. 61) destacam a temática do acesso de conteúdo e provas existentes em contas remotas ou nos chamados serviços de nuvem, que demanda autorização judicial, questionando a licitude da prova em detrimento da premissa constitucional de *nemo tenetur se detegere* ou de que ninguém é obrigado a fazer prova contra si mesmo (art. 5º, LXXX, CF), e relatando que, diante do avanço tecnológico e da utilização crescente das novas tecnologias, há a necessidade de se encontrar o equilíbrio entre a preservação da intimidade e a coleta de provas digitais sob o resguardo de autorização judicial.

Nesse sentido, no que tange a provas digitais originadas de ambientes em nuvem computacionais, há ainda peculiaridades quanto as suas características de imaterialidade, volatilidade e dispersão geográfica, inexistindo na legislação pátria regramento sobre meios específicos de obtenção de prova digital (MINTO, 2021. p. 34-36).

Essas peculiaridades evidenciam a diferença entre o repositório (local físico) e os dados nele contidos. É outro aspecto importante com o qual se tem de lidar, porque a Tecnologia da Informação se torna acessível por meio da estrutura da Internet, e essa é representada por computadores, atualmente disponíveis em variados tipos de aparelhos, desde *notebook*s até aparelhos de telefonia celular – isso em termos de formas disponibilizadas para a população em geral.

Do ponto de vista técnico, para além da extraterritorialidade, a crescente utilização de soluções disruptivas e de armazenamento de dados em plataformas de computação em nuvem envolve desafios para coleta, processamento e preservação de evidências digitais *in loco*. Esses desafios se devem às dificuldades de se extrair e de se manter custódia digital de um elevado quantitativo de massa de dados (*big data*) e à limitação legiferante no sentido das particularidades da cadeia de custódia. Hoje, mesmo após o advento do pacote anticrime, essa cadeia se concentra apenas no fluxo processual e na cadeia de custódia de evidências físicas (MINTO, 2021, p. 55).

Nesse cotejo, Dário José Kist (2019 apud MINTO 2021, p. 56) considera que a prova digital deveria ser objeto de regime jurídico autônomo, que contemplasse regras sobre a obtenção dos diversos meios de prova digital e garantias de fidedignidade na recolha e preservação da cadeia de custódia, elaboradas a partir das especificações do mundo digital.

Nesse contexto, principalmente de morosa tramitação legislativa, a aplicação de modelos regulatórios para obtenção e guarda de provas digitais (cadeia de custódia digital), por meio de uso de tecnologias disruptivas, pode ser uma alternativa viável para enfrentar os riscos jurídicos aventados, norteando o operador do Direito e seus auxiliares (peritos judiciais, por exemplo) sobre como proceder. Baptista e Keller (2016, p. 174) afirmam que a regulação das inovações disruptivas, para além do reconhecimento, “traz segurança para que as atividades se desenvolvam sob o amparo do direito”.

Nessa perspectiva, a autorregulação à sombra do Estado (*under the shadow of the State* – em tradução literal) revela um incentivo institucional à autorregulação sob a ameaça de intervenção estatal caso não se alcancem resultados esperados (Kleinsteuber, 2004 apud Aranha, 2023, p. 91), podendo ser um importante meio para convergência regulatória de cadeia de custódia de provas digitais, haja vista que a nuvem computacional é global, transcende jurisdições e supre a morosidade legislativa a despeito do surgimento de novas tecnologias.

Nesse cotejo, uma proposição sugerida específica para a cadeia de custódia digital seria a adoção de critérios internacionais já acreditados e abarcados pela convenção de Budapeste e pelas *Big Techs* para atendimento de legislações supranacionais, como critérios mínimos que podem ser valorados na admissibilidade e na acreditação de provas digitais, centrados no Conselho Nacional de Justiça (CNJ), a título exemplificativo.

A questão que se coloca neste momento é que, se por um lado, o Direito digital tem como princípio normativo a autorregulação, dadas as constantes evoluções tecnológicas e a extraterritorialidade do ciberespaço (PINHEIRO, 2021, p. 121), por outro, urge a necessidade de estabelecimento de procedimentos técnicos bem delineados que possibilitem: resguardar os princípios jurídicos atinentes à prova colhida e mantida em meio digital, assegurando os fundamentos basilares de garantia da informação – confidencialidade, integridade, disponibilidade e não repúdio (ABNT/NBR 27001, 2013) – com o estabelecimento de uma cadeia de custódia de prova digital (ABNT/NBR 27037, 2013); proporcionar a acreditação e a admissibilidade da prova digital na esfera judicial.

Ressalva Lorenzo Parodi (2021, p. 3) que definir em lei procedimentos técnicos relativos à cadeia de custódia de evidências digitais pode ser inútil ou contraproducente, já que, em um ambiente de rápida e de constante evolução tecnológica, há uma grande chance de tais procedimentos serem rapidamente ultrapassados, ficando em desacordo com as melhores práticas.

Em contrapartida, Aranha (2023, p. 68) ressalta que a teoria de autorregulação regulada parte do pressuposto de que as empresas são, de fato, mais capazes de regular suas atividades empresariais do que o governo. Isso é o que já ocorre com as *Big Techs (e.g*. Microsoft, Google, Facebook), que, para dirimir constantes requisições das mais diversas autoridades policiais nos países em que prestam seus serviços,

optaram por definir um padrão de comunicação com os órgãos competentes e por desenvolver mecanismos e ferramentas voltados à temática investigativa.

Nesse cotejo, exemplifica-se o sistema LERS (2023), acrônimo para *Law Enforcement Request System,* desenvolvido pelo Google para requisitar, monitorar e acompanhar o atendimento das demandas das autoridades públicas na seara de acesso, interceptação e/ou bloqueio de usuários da referida empresa.

Nessa seara, também referencia-se documento de apoio desenvolvido pela referida *Big Tech* para nortear o formato com que os pedidos devem ser encaminhados no sistema e consolidar as dúvidas comuns (LERS-FAQ, 2023).

Se, por um lado, a iniciativa do provedor de serviços de nuvem (*cloud service provider*, em tradução livre) de autorregular seu próprio serviço possa ser visto como uma forma positiva de melhor atendimento dos aspectos de conformidade legal, transparência e prestação de contas com seus usuários, por outro, acaba por restringir a atuação das autoridades, entre o que se espera e o que a empresa se propõe a entregar, conflitando interesses econômicos e se apoiando no Direito Internacional para justificar a extraterritorialidade e/ou o não cumprimento integral da legislação brasileira.

Ocorre que a ausência de regulação mercadológica e a complexidade de envolvimento e adequação aos mais diversos mecanismos legais dos países em que tais empresas atuam acabam por impactar na melhor tratativa para atendimento dos casos utilizando-se como base a Lei Cloud norte-americana e os tratados internacionais vigentes e trazendo a responsabilidade de adequação legal ao Estado e não à empresa.

Essa é a problemática evidenciada neste trabalho, que destaca três pontos de interesse para aprofundamento, considerados bastante sensíveis ao atual combate aos crimes cibernéticos: computação em nuvem, evidências digitais e regulação. Esses pontos estão relacionados entre si.

O objetivo deste estudo é avaliar o instituto da regulação na esfera administrativa (autorregulação) como meio de assegurar padrões de confiabilidade à cadeia de custódia de evidências digitais obtidas em ambientes de nuvem computacional. Em última instância, visa-se à admissibilidade de evidências digitais como prova em cibercrimes.

A abordagem do tema é relevante, antes de tudo, por ser oportuna em relação aos descompassos legais observados frente ao exponencial número de ocorrências criminosas envolvendo o ambiente virtual. Também porque se trata de uma temática de interesse geral, haja vista a tecnologia permear o cotidiano de todos, desde as relações pessoais até as relações institucionais; a tecnologia vem proporcionando facilidades nesse sentido. Conhecer as reais implicações do trabalho dos operadores do Direito e da busca de soluções do judiciário para assegurar a tutela dos direitos dos cidadãos é fundamental para não se perder a crença na justiça.

Metodologicamente, o trabalho foi desenvolvido na perspectiva do Direito Comparado, com inserções no Direito dos Estados Unidos e da União Europeia, a fim de situar a legislação brasileira em relação a duas visões diferentes, resguardados os respectivos contextos. A abordagem foi eminentemente qualitativa, tendo em vista a proposta do trabalho.

Relativamente aos procedimentos metodológicos, a pesquisa se classifica como bibliográfica, porque foi desenvolvida por meio de uma revisão da literatura com consulta a publicações nacionais e internacionais sobre o tema, incluindo a legislação pertinente, quando foi o caso.

O trabalho encontra-se estruturado em quatro capítulos, abrangendo os seguintes pontos: no primeiro, apresenta-se a fundamentação teórica da pesquisa, iniciando-se pela relação entre Internet, tecnologia, Direito e regulação no ambiente virtual, como forma de demonstrar a inter-relação entre essas temáticas. Foram discutidos dois dos pontos integrantes do tripé de sustentação da pesquisa, especificamente computação em nuvem e evidências digitais, e descritos aspectos fundamentais diretamente associados ao objetivo do estudo, a exemplo dos problemas de jurisdição em crimes cibernéticos praticados na computação em nuvem.

No segundo, o foco está em evidenciar as condições da legislação brasileira em termos de atualização, face à computação em nuvem e da obtenção de provas digitais. Também são levantados pontos de convergência entre o Direito Internacional Público e o Direito Internacional em relação aos crimes cibernéticos.

No terceiro, discute-se a acreditação e a admissibilidade das provas digitais no judiciário brasileiro, a confiabilidade dos dados em ambiente de computação em nuvem e as propostas de projetos de lei em tramitação.

No quarto e último capítulo, aborda-se a regulação como forma de acreditação e de admissibilidade das evidências digitais no judiciário brasileiro, o terceiro pilar do tripé da pesquisa. É uma abordagem teórica e contextualizada em relação à função do Estado regulador e às normas internacionais referentes à temática das evidências digitais. Estão descritos requisitos mínimos para a acreditação e evidências digitais com base no Direito Comparado.

1 FUNDAMENTAÇÃO TEÓRICA

A sociedade atual vivencia uma nova estrutura social, na qual a Tecnologia da Informação (TI), aliada à massificação de uso da Internet, acaba se inserindo intrínseca e definitivamente no cotidiano de todas as áreas da vida, modificando hábitos, costumes, formas de convívio social e realização de negócios. Com isso, modificou as características da sociedade e se tornou um campo fértil para o desenvolvimento econômico.

O conhecimento gerado pela TI levou ao desenvolvimento de um paradigma técnico-econômico, no sentido literal definido por Thomas Kuhn (1988, apud SILVA NETO, 2011, p. 347): uma estrutura composta de teorias, de métodos, de instrumentos e de experiências, “que serve para o pensamento organizar, de determinado modo, a realidade e os seus eventos. Essa estrutura [...] é assumida e partilhada pelo conjunto dos membros da comunidade científica”.

A Internet tem um papel fundamental nesse contexto, por fornecer a estrutura necessária à disseminação e ao compartilhamento da TI. A Internet e o acesso à TI são contabilizados pelo uso de computadores e/ou dispositivos conectados” (COMENALE, 2018, p.4). Apenas para ilustrar o funcionamento dessa estrutura de forma direta, a Internet, uma rede mundial gigante de computadores, interliga entre si tanto grandes computadores como *notebooks* e computadores pessoais por meio de telecomunicações, incluindo desde linhas de telefone comuns, linhas privadas de comunicação, até canais de satélite e cabos submarinos. Essa comunicação se dá via Protocolo de Controle de Transmissão (TCP), responsável pela transmissão de dados, associado ao Protocolo de Internet (IP), indentificador de computadores e de servidores (CIN/UFPE, 2023, p. 1). Esse aparato estrutural e seu vasto número de meios de comunicação funciona em sistema local e em sistema de nuvem.

Nesse cotejo, Guilherme Damásio Goulart (2012, p. 146 apud PEREIRA FILHO *et al.*, p. 46) considera que a expansão do uso das novas tecnologias impacta todas as áreas da ciência jurídica.

Cabendo ao Direito fornecer as diretrizes de funcionamento da vida social neste novo paradigma que, sem trazer novos direitos, exige novos meios de assegurar sua tutela.

Nesse sentido, compreender minimamente as premissas da Internet, cuja estrutura permeia o conhecimento via TI, e não só, é fundamental para se dimensionar as dificuldades com as quais o Direito, principalmente o Direito Penal, está se defrontando.

1.1 Internet, tecnologia e direito no ambiente virtual

O mundo da comunicação evoluiu exponencial e irreversivelmente com o surgimento da Internet, permitindo que o indivíduo se exponha na grande rede e abrindo espaço para novos instrumentos de comunicação, como as redes sociais.

O advento da Internet e das tecnologias digitais fez emergir uma nova forma de organização social, política e econômica denominada “sociedade da informação”, descrita largamente pelo sociólogo espanhol Manuel Castells (1999) em suas pesquisas sobre os reflexos da sociedade em rede na economia moderna.

Werthein (2000), citando Castells, explica que o paradigma em que se insere esta sociedade é regido pelas seguintes características fundamentais, associadas à reestruturação e, concomitantemente, à expansão do capitalismo:

> • a informação é sua matéria-prima: as tecnologias se desenvolvem para permitir o homem atuar sobre a informação propriamente dita;
> [...]
> • os efeitos das novas tecnologias têm alta penetrabilidade porque a informação é parte integrante de toda atividade humana, individual ou coletiva e, portanto todas essas atividades tendem a serem afetadas diretamente pela nova tecnologia;
> [...]
> • predomínio da lógica de redes, característica de todo tipo de relação complexa, que pode ser, graças às novas tecnologias, materialmente implementada em qualquer tipo de processo;
> • flexibilidade: a tecnologia favorece processos reversíveis, permite modificação por reorganização de componentes e tem alta capacidade de reconfiguração;

> • crescente convergência de tecnologias, principalmente a microeletrônica, telecomunicações, optoeletrônica, computadores, mas também e crescentemente, a biologia. O ponto central aqui é que trajetórias de desenvolvimento tecnológico em diversas áreas do saber tornam-se interligadas e transformam-se as categorias segundo as quais pensamos todos os processos (WERTHEIN, 2000, p. 72).

Somem-se a essas caraterísticas seus desdobramentos, suas inter-relações, as peculiaridades das descobertas mais recentes – tendo em conta o tempo decorrido entre aquelas descritas e o ritmo intenso da evolução da TI – e os efeitos negativos desse conjunto, então tem-se o ambiente atual.

Nesta nova sociedade, a informação foi promovida ao posto de principal riqueza, por ter se tornado “indispensável ao desempenho de qualquer atividade”. O uso da TI se intensificou em todos as áreas da vida em quantidade e em qualidade, interligando todos os processos tecnológicos por meio de uma linguagem e de uma interface comuns. Com essa linguagem e nessa interface, “a informação é gerada, armazenada, recuperada, processada e transmitida”. Nessa forma nova, a organização social se utiliza intensamente da Tecnologia da Informação como instrumento que facilita os processos de produção, processamento, transmissão, armazenamento e coleta de informações (VIEIRA, 2007, p. 157).

As transformações decorrentes dessa nova realidade são imensuráveis e geraram, em grande escala, outras formas de relações sociais e jurídicas que funcionam como parâmetro das relações de poder no mundo contemporâneo (PINHEIRO, 2021, p. 68). A evolução da TI possibilitou a internacionalização das relações humanas, tornando relativas as distâncias geográficas e possibilitando múltiplas e instantâneas interações. A transnacionalidade do direito é uma consequência deste desenvolvimento, pois ela emerge do emaranhado entre Direito, sociedade, novas tecnologias e novos modelos econômicos, em vez de manifestar-se simplesmente como um Direito que emerge do Estado (CAMPOS, 2022, p. 40).

Para além dos benefícios tecnológicos, econômicos e sociais, a evolução da tecnologia trouxe novos riscos, novos campos de exploração criminosa, novos meios de execução e condutas que tornaram o ambiente virtual uma “terra fértil” para as mais diversas práticas, tanto lícitas como ilícitas (PINHEIRO, 2021, p. 63-64). Ao vasto incremento das relações sociais – como as novas formas de contato a qualquer

distância e em tempo real, por exemplo – contrapõem-se concomitantes complicações e problemas, a exemplo da criação de uma zona criminógena igualmente vasta em fins, em meios e em sofisticação. Qualitativamente, a mesma sofisticação que beneficia e facilita a vida da sociedade põe em alerta suas rotinas.

Este novo contexto social revolucionou as relações jurídicas, da mesma forma que aconteceu com a Revolução Industrial, quando o desenvolvimento tecnológico alterou as formas de relação social e de trabalho, principalmente. Assim, a sociedade da informação não se restringe ao ambiente virtual; as relações interpessoais da sociedade industrial, seus direitos e deveres continuam. A eles, a sociedade da informação acrescentou um nível de produtividade maior nos processos de manuseio e de tratamento de dados das diversas áreas por meios eletrônicos. Em vista disso, o Direito em geral foi afetado (COMENALE, 2018, p. 3).

O Direito acompanha os movimentos da sociedade e inseriu-se na era digital menos por inovação e mais por necessidade. Para tanto, busca a inserção de mecanismos que funcionem no sentido de estabelecer a ordem social, seu objetivo. Por meio da Internet, ele tem possibilidade de assegurar relações jurídicas diversas, em trânsitos que se intensificam entre o mundo digital e o real. Pelo menos aparentemente, a informação digital tem dado certa estabilidade a essas relações, pela facilidade de acesso da população que se utiliza do sistema judiciário do mundo digital. Discussões e avanços referentes à regulação de assuntos relativos à informática representam exemplos “de como o Direito, como mecanismo de controle social, teve (e cada vez mais terá) que se adaptar e ampliar seus estudos” para as ocorrências do mundo virtual. Ramos do Direito Público, por exemplo, tratam de questões da sociedade da informação não apenas no campo processual. Porém, o ramo que mais fica em destaque talvez seja o Direito Penal, pela ocorrência de “crimes cibernéticos”, crimes informáticos ou crimes eletrônicos (COMENALE, 2018, p. 3).

1.1.1 Condições do ambiente real: aspectos gerais

O Direito Penal, especificamente, vem encontrando dificuldades de adaptação a este novo paradigma técnico-econômico. “O Direito em si não consegue acompanhar o frenético avanço exponencial proporcionado pelas novas tecnologias, em especial pela Internet”, que criou um ambiente virtual totalmente livre e sem fronteiras. Esse ambiente acoberta novas modalidades de crimes, na chamada “criminalidade virtual”, praticada por indivíduos que se aproveitam da ausência de regras e se utilizam das possibilidades de anonimato (GIMENES, 2013, p. 3).

Nesse sentido, Tavares Neto e Kozicki (2008) ratificam a necessidade de atualização epistemológica, metodológica e paradigmática, que englobe a releitura do direito constitucional num referencial crítico e interdisciplinar, que considere os direitos humanos, o meio ambiente e o direito penal internacional como categorias de análise do próprio direito, na função de instrumental regulatório nas sociedades contemporâneas.

De início, considera-se que, no mundo jurídico, é relevante a distinção entre o ambiente interno e o externo, seja na concessão de direitos, na regulamentação de questões de natureza cível ou tributária, seja na definição das pessoas jurídicas ou dos assuntos ligados à soberania de um determinado país.

No ambiente virtual da Internet, no entanto, o conceito de interno e externo sofre uma inversão: interno é o que está na rede, e externo aquilo está fora dela. Tal característica traz uma reflexão sobre o conceito de liberdade que, na definição comum dos Estados de Direito, está relacionada com a faculdade de fazer aquilo que não é proibido na lei nacional. Essa distinção se mostra relevante, porquanto o que pode ser crime em um Estado, por haver lei que o veda, pode não o ser em outro. Nessa perspectiva, em se tratando de ambiente virtual, onde se inicia um Estado e termina o outro? (PINHEIRO, 2013, p. 51). Os cibercrimes, na grande maioria das vezes, se caracterizam por serem plurilocais, quando vítima e agenda estão em locais distintos, ou ainda, quando a execução do delito tem início em um lugar e a consumação ocorre em outro (BARRETO, 2016, p. 25).

Em Estados com viés totalitário, que mantêm vigorosas legislações de controle dos meios de comunicação e sobre a liberdade de expressão, é relativamente simples

controlar uma rede física inserida no espaço político de um país. Entretanto, como controlar a Internet por meio de instrumentos de coerção estatal se o espaço da rede, ao menos em tese, não suporta fronteiras?

A intangibilidade e a mobilidade das informações armazenadas e transmitidas pela Internet, atreladas à fugacidade e à instantaneidade com que as conexões são estabelecidas e encerradas, aliadas à possibilidade de não exposição física do usuário e ao alcance global da rede, são peculiaridades da rede. E isso que caracteriza o ambiente virtual da tecnologia também é o que dificulta a ação jurídica, no que tange a aspectos como obtenção de provas, por exemplo. Em complemento, a ação da justiça ainda possui características relacionadas à soberania estatal: territorialidade (local da ação criminosa), população (pessoas atingidas), poder sobre o território (onde o crime ocorreu e onde as pessoas estavam) e reconhecimento (do problema para uma ação consensual).

Na visão de Castells (2007), a noção de Estado Nacional deve ser redimensionada para abranger as relações no ambiente virtual como extensão de seus próprios territórios, sem que isso implique perda de soberania:

O Estado não desaparece. É apenas redimensionado na Era da Informação. Prolifera sob a forma de governos locais e regionais que se espalham pelo mundo com seus projetos, formam eleitorados e negociam com governos nacionais, empresas multinacionais e órgãos internacionais. O que os governos locais e regionais não têm em termos de poder e recursos é compensado pela flexibilidade e atuação em redes (CASTELLS, 2007, p. 203).

Nessa perspectiva, com vistas a envidar esforços no combate aos crimes eletrônicos, a chamada Convenção de Budapeste ou Convenção sobre o Cibercrime, de 23 de novembro de 2001, tipificou os principais crimes praticados na Internet, partindo da premissa de que o combate aos crimes virtuais deve embasar-se em um regime internacional. Isso porque, segundo Castells (2007, p. 203), o crime global, a formação de redes entre poderosas organizações criminosas e seus associados, com atividades compartilhadas em todo o planeta, constitui um novo fenômeno que afeta profundamente a economia no âmbito internacional e nacional, a política, a segurança e, em última análise, as sociedades em geral.

A Convenção de Budapeste – à qual o Estado brasileiro aderiu recentemente

por meio do Decreto n. 11.491/2023, cerca de 22 anos depois de sua promulgação – conta com mais de sessenta países signatários e busca uniformizar atuações legislativas de crimes cibernéticos, a fim de possibilitar punições aos infratores de modo transnacional, mitigando conflitos entre legislações no espaço (PINHEIRO, 2023, p. 1).

Nesse sentido, antes da adesão do Brasil a essa Convenção, apenas a Lei n. 12.735/2012 – que tipificou condutas realizadas por meio de sistemas eletrônicos, digitais ou similares, praticadas contra sistemas informatizados e similares, – e a Lei n. 12.737/2012 – que estabeleceu a tipificação criminal de delitos informáticos, alterando o Código Penal – aproximaram o país da modernização legal no enfrentamento desse tipo de crime.

Na lição de Patrícia Peck Pinheiro (2023), o Decreto n. 11.491/2023 permite não só evoluir com o que tem de ir para o Congresso para fazer adaptações na legislação nacional, mas regulamenta a utilização de importantes princípios de cooperação e de assistência mútua previstos nos arts. 23 e 25, e da própria informação espontânea, prevista no art. 26 da convenção de crimes cibernéticos.

Nessa perspectiva, mesmo ante a vasta codificação penal e processual penal do país, a todo momento surgem técnicas delitivas que não se encaixam na tipificação penal vigente. Desse modo, para cuidar da nova realidade, faz-se necessária uma legislação atualizada.

1.2 Crimes cibernéticos e características conceituais

No Brasil, escolheu-se nomear os crimes cometidos contra a informática de “delitos informáticos”, termo usual em países de língua espanhola que se relaciona à ideia de proteção de objeto jurídico “informática e informação” (JESUS; MILAGRE, 2016, p. 49). No entanto, as denominações variam bastante, bem como os tipos de crimes que elas abarcam, indicando certa falta de consenso. Por isso, é importante conhecer um pouco de como esse crime vem sendo tratado conceitualmente.

Autores referidos por Gimenes (2013, p. 3, 5) definem o crime nessa área de forma ampla – “(é) o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por

objeto material ou meio de execução o objeto tecnológico informático (*hardware*, *software*, redes, etc.)" (Feliciano, 2000) – e de forma mais restrita – "um ato lesivo cometido por meio de um computador ou de um periférico com a intenção de se obter uma vantagem indevida" (Nigri, 2000). Na perspectiva da Organização para a Cooperação Econômica e Desenvolvimento (OCDE), é qualquer conduta antiética, ilegal ou sem autorização que implique processamento e/ou transmissão de informações ou dados. Em resumo, é ação antijurídica, típica e culpável contra alguém, realizada com o uso de meios informáticos, tendo o computador ligado à Internet como instrumento.

Rossini (2004) define delito informático como a conduta do praticante, típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica com o uso da informática, em ambiente de rede ou fora dele. Essa conduta ofende direta ou indiretamente a segurança da informação, cujos elementos são: integridade, disponibilidade e confidencialidade. Essa denominação de Rossini, segundo Gimenes (2013, p. 3), inclui crimes e contravenções penais, alcançando todas as condutas relacionadas com sistemas de informática, seja como meio, seja como fim, "delitos em que o computador seria uma mera ferramenta, sem a imprescindível 'conexão' à Rede Mundial de Computadores ou a qualquer outro ambiente telemático". Nessa ideia, o "delito informático" é gênero, e o "delito telemático" é espécie, devido à condição de se dar "no e a partir do inter-relacionamento entre os computadores em rede telemática usados na prática delitiva".

Patrícia Peck Pinheiro (2016, p. 307) define e pontua juridicamente o cibercrime: "crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual". Ou seja, ele é operacionalizado em ambiente virtual e produz efeitos no mundo real. Esses crimes são classificados como impuros ou impróprios, a exemplo dos crimes previstos no Código Penal (CP): induzimento, instigação ou auxílio a suicídio (art. 122); de calúnia, difamação e injúria (arts. 138 a 140); de ameaça (art. 147); de divulgação de segredo (art. 153); de extorsão (art. 158); e de estelionato (art. 171).

Todavia, com a evolução da Tecnologia da Informação, surgiram os "crimes-fim", aqueles praticados com finalidades totalmente digitais, tipificados na legislação penal brasileira por meio das chamadas Leis de Crimes Digitais, as referidas Leis n.

12.735/2012 e n. 12.737/2012. Eles são classificados como crimes cibernéticos puros ou próprios e têm como exemplo as seguintes ações, também previstas no Código de Processo Civil (CPC): invasão de dispositivo informático (art. 154-A); inserção de dados falsos em sistemas de informações (art. 313-A); e modificação ou alteração não autorizada de sistema de informações (art. 313-B).

Como se vê, mesmo não havendo legislação específica, condutas tidas como crimes virtuais estão tipificadas em textos legislativos como o CP e em leis esparsas. E diferentemente do que se afirma, aplicar a lei vigente a tais crimes não representa analogia, uma vez que não se trata de crimes novos, pois não há novos bens jurídicos a serem tutelados. O novo, nesse tipo de criminalidade, é o *modus operandi*, a forma como os criminosos se utilizam das tecnologias (GIMENES, 2013, p. 5).

1.2.1 Local do crime e limites de jurisdição

A sociedade de informação, com as características que a definem, advindas da TI – as citadas instantaneidade, fugacidade e o que delas deriva –, de certa forma, não tinha como manter intactas categorias tradicionais, a exemplo da noção de lugar e, obviamente, seus limites. Dessa forma, redefinições e ressignificações são feitas (SOUZA, 2021, p. 30), sempre à luz de como tais características se apresentam, senão na realidade concreta, na realidade virtual.

Para André L. M. Lemos (1996 apud GIMENES, 2013, p. 4), “no ciberespaço, há transcendência da matéria”. A noção de geografia que se conhece deu lugar a outra, que é real, mesmo não sendo material. “O ciberespaço é um não lugar, “ao qual só se tem acesso via computador. É uma realidade na medida em que é utilizado diariamente, como intermediador entre os mundos real e virtual.

O ciberespaço faz parte do processo contemporâneo de desmaterialização do espaço e de instantaneidade temporal, após dois séculos de industrialização moderna que insistiu na dominação física de energia e de matérias e na compartimentalização do tempo. Se na modernidade o tempo era uma forma de esculpir o espaço, com a cibercultura contemporânea nós assistimos a um processo em que o tempo real vai aos poucos exterminando o espaço (LEMOS, 1996, apud GIMENES, 2013, p. 4).

Essa noção explica por que um dos maiores desafios na computação forense

é a identificação exata dos locais de um cenário criminoso determinado, cuja principal pista é a informação digital. A correta identificação, o isolamento, a coleta e a preservação de vestígios de natureza digital são fatores imprescindíveis para a perseguição da autoria e para a comprovação da materialidade do crime.

Determinar territorialidades implica determinar o juiz competente para processar e para julgar o delito informático. Em qualquer país, o Direito nacional se restringe à sua área territorial. Logo, o Direito Penal brasileiro se volta para o território brasileiro, e o que ocorre fora de tais limites resulta em revisão dos acordos entre os países, conforme norteiam os arts. 5º a 7º do Código Penal.

No primeiro momento, considera-se que o CP brasileiro adotou, em seu art. 6º, a teoria da ubiquidade para referenciar o local do crime, considerando lugar do crime o local em que ocorreu a ação ou a omissão no todo ou em parte, bem como onde foi produzido ou deveria ser produzido o resultado. Sendo assim, v. g., ao considerar que alguém no estado do Rio de Janeiro invadiu o computador de outrem, localizado em São Paulo, o juízo competente para processar e julgar o delito informático seria aquele no qual se encontra o dispositivo invadido (JESUS; MILAGRE, 2016).

Contudo, tecnologias que dificultam a identificação do atacante – como redes virtuais privadas (VPN), *proxies* e outros dispositivos de mascaramento de endereços do Internet Protocol (IP) –contribuem para mascarar dados de um criminoso que comete crimes em território nacional, ao indicarem a origem do ato criminoso em equipamentos alocados no exterior. Esse disfarce na indicação dificulta a identificação/localização real do criminoso e envolve outras nações soberanas no processo investigativo.

Uma opção nesse sentido é o que defendem Jesus e Milagre (2016), quanto a se adotar, em crimes da Internet, algo semelhante à teoria da atividade, determinando como local do crime aquele em que o agente praticou o delito. Valin (2000) considera local do crime aquele em que está o autor das infrações, pois o respectivo país teria melhores condições de punir. Já Zaccaria de Inellas (2009) posiciona-se no sentido de que se deve aplicar a regra geral do art. 6º do CP, teoria da ubiquidade, sem prejuízo de convenções, tratados e regras de Direito Internacional. Assim, os delitos cometidos fora do território nacional podem aqui receber punição se previstos em convenções/tratados dos quais o Brasil é parte.

Pelos termos do §2º do art. 70 do Código de Processo Penal, quando atos executórios tiverem ocorrido fora do Brasil, a competência será do local em que a infração se deu ou foi concluída a ação delituosa (resultado). Já o art. 7º, II, § 2º, “a” e “b”, do CP dispõe que, nos casos de crimes praticados por brasileiros no exterior com vítimas no Brasil, por questões de soberania, a conduta deve ser considerada ilícita em ambos os países. O agente deve retornar ao território nacional para ser processado.

Nesse sentido, independentemente dos posicionamentos pessoais ou de grupo, a doutrina é uníssona ao tratar da necessidade de se firmar um documento internacional que aponte parâmetros globais a serem observados, com o fito de se evitar o entendimento de que todos os países – ou nenhum deles – se considerem aptos a julgar referidos crimes. É dentro dessa perspectiva que os meios e os procedimentos para coleta e para a preservação de evidências digitais ganham especial importância e destaque. E não só: tornam-se essenciais, se se considerar que da admissibilidade de tais evidências como prova de crimes cibernéticos é que dependem as soluções buscadas.

1.3 Nuvem computacional: “a virtualização dos *data centers*”

A nuvem computacional é uma tendência recente nas Tecnologias da Informação, e o termo “nuvem”, naturalmente, é uma metáfora. Significa um modelo para permitir acesso à rede onipresente, de forma conveniente e sob demanda, a um conjunto compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços), os quais podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou interação com o provedor de serviços. Significa ainda que, para utilizar os serviços, basta que o usuário tenha em sua máquina um sistema operacional, um navegador e acesso à internet. (KIST, 2019 apud MINTO, 2021, p. 36).

Do ponto de vista da palavra em si, “nuvem” suscita a ideia de algo distante, de que só se vê o início e o fim, desconhecendo-se o interior, seu ambiente. Por isso, considera-se que o uso do termo como nomenclatura foi bem apropriado, pois toda a infraestrutura e os recursos de computação “ficam escondidos”. O usuário apenas acessa “uma interface padrão”, por meio da qual são disponibilizados os serviços e as

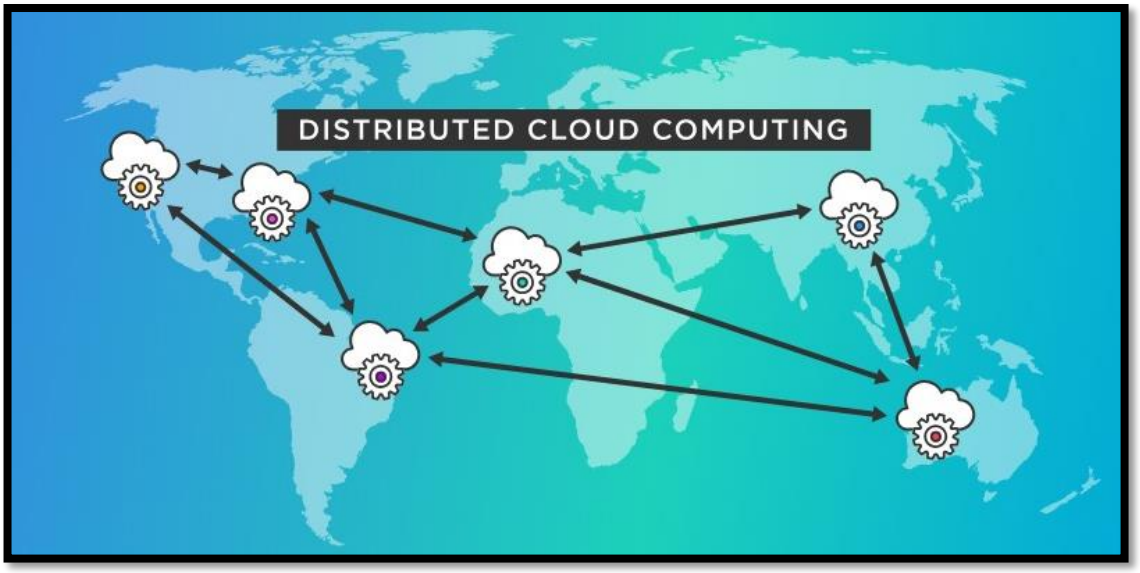
aplicações (PEDROSA; NOGUEIRA, 2011, p. 1).

Trata-se de um novo modelo de computação que permite ao usuário final acessar uma grande quantidade de aplicações e serviços em qualquer lugar e independentemente da plataforma, bastando um terminal conectado à “nuvem”. A nuvem é representada pela internet, isto é, a infraestrutura de comunicação composta por um conjunto de *hardwares, softwares*, interfaces, redes de telecomunicação, dispositivos de controle e de armazenamento que permitem a entrega da computação como serviço (PEDROSA; NOGUEIRA, 2011, p. 1).

Segundo os autores, para a execução desse modelo, todos os dados e todas as aplicações dos usuários são reunidos em centros grandes de armazenamento, os *data centers*. Após a reunião, tanto a infraestrutura como essas aplicações são distribuídas em forma de serviços disponibilizados na Internet. Taurion (2008, p. 2) esclarece: “o resultado é que a nuvem pode ser vista como o estágio mais evoluído do conceito de virtualização, a virtualização do próprio *data center*.”

A computação em nuvem leva o conceito de sistema distribuído ao ponto extremo, disponibilizando, inclusive, plataformas de *software* e *hardware* sob demanda, para atender às necessidades individuais ou empresariais, de forma transparente ao usuário final (ARRUDA, 2013, p. 6-7). Na topologia atual de nuvem computacional distribuída, não existe um ponto central (*hub*) que concentre dados (como se visualiza no exemplo simplificado da Figura 1 a seguir), de forma que um terminal-cliente pode se comunicar com muitos servidores ao mesmo tempo, trocando informações entre si.

Figura 1 - Distribuição de dados na computação em nuvem



Fonte: TIBCO (2023)

A nuvem computacional pode ter uma ou mais centrais de gerenciamento, constituídas por vários provedores de serviços (*cloud service providers*), que administram diferentes domínios, como o Google – que administra o Gmail –, o Office 365, entre outros. Novas funcionalidades para aplicações e serviços podem ser disseminadas a partir de uma central administrativa, sem que o consumidor tenha que se preocupar com a complexidade de gerenciamento do ambiente (KIST, 2019 apud MINTO, 2021, p. 36), dentre as maiores destacam-se a Amazon Web Service (AWS), a Microsoft Azure e a Google Cloud Platform (GCP).

Além de prestar serviços, a computação em nuvem corrige a grande ociosidade de equipamentos e de *softwares*, relativa ao tempo sem uso. É que a computação em nuvem trabalha sob demanda, contabilizando os serviços de forma semelhante ao consumo de energia e de telefone, por exemplo. Então, frente a todas as implicações da prestação de serviços de tecnologia, essa computação representa uma alternativa bastante positiva, “pois aloca recursos computacionais à medida que eles sejam demandados. Se houver maior demanda de transações, mais recursos são alocados. Se a demanda diminuir, esses recursos são liberados para outras aplicações”. Em consequência, podem-se inserir ou excluir dados instantaneamente, o que termina por se associar objetivamente ao trabalho por demanda, como explicam Ramos e Farias Júnior (2010, p. 3), citando Taurion (2009).

São três tipos de nuvem – públicas, privadas e híbridas –, com características semelhantes, mas com diferenças que atendem às peculiaridades e às necessidades do cliente. O funcionamento é basicamente igual, uma vez que têm o mesmo objetivo. As nuvens se dividem em áreas distintas: *Infrastructure as a Service* (IaaS), infraestrutura como serviço, conforme a demanda do contratante; *Plataform as a Service* (PaaS), plataforma, serviços na web e armazenamento de informações em bancos de dados; *Software as a Service* (SaaS), *software*s utilizados via web, a exemplo dos aplicativos do Google (RAMOS; FARIAS JÚNIOR, 2010, p. 3).

De modo geral, o funcionamento dos serviços na nuvem de computação é simples: “as informações são armazenadas em *data centers* localizados em qualquer lugar do mundo e mantidos por terceiros” (como demonstrado na Figura 1). Os dados ficam em servidores hospedados e podem ser acessados facilmente por meio de uma interface web. O servidor ao qual o acesso se conecta direciona os dados para outros, localizados em um ou mais *data center*, de acordo com o “tamanho da operação do

provedor de nuvem” (ARQUIVEI, 2023, p. 1).

Mas a computação em nuvem tem desafios e desvantagens. Um dos principais desafios apontados foi a absorção dessa nova cultura por parte de organizações e de profissionais conservadores nessa área. Outro desafio diz respeito às IaaS, PaaS e SaaS e às respectivas buscas para identificar de que forma cada uma dessas áreas pode auxiliar o contexto das organizações em particular. Vê-se que esses desafios estão voltados para a computação em nuvem como auxiliar de negócios, não como serviço de tecnologia (RAMOS; FARIAS JÚNIOR, 2010, p.5-6).

Quanto às desvantagens, elas representam pontos-chave para a evolução da computação em nuvem: segurança, escalabilidade, interoperabilidade, confiabilidade e disponibilidade (PEDROSA; NOGUEIRA, 2011, p. 2-3). A descrição desses pontos é importante para os objetivos deste trabalho, porque, em certa medida, demonstrando-se as fragilidades das nuvens, demonstram-se também as condições em que possíveis pistas criminosas podem ser identificadas.

A *segurança* é o desafio mais visível a ser enfrentado, pois a informação antes armazenada localmente estará na nuvem em local físico sem precisão de onde fica nem de que tipos de dados nela estão armazenados. A privacidade e a integridade das informações são então itens de suma importância, pois, especialmente em nuvens públicas, existe uma grande exposição a ataques.

A *escalabilidade* é uma característica fundamental na computação em nuvem, pois as aplicações para uma nuvem precisam ser escaláveis (ou “elásticas”). Dessa forma, os recursos utilizados podem ser alterados conforme a demanda. Para que isso seja possível, as aplicações e seus dados devem ser flexíveis o suficiente.

A *interoperabilidade* é o fator que consiste na capacidade dos usuários de executar seus programas e seus dados em nuvens diferentes, permitindo assim que eles não fiquem restritos somente a uma nuvem.

A *confiabilidade* está relacionada à frequência com que o sistema falha e ao impacto de suas falhas (perda ou não dados). As aplicações desenvolvidas para computação em nuvem devem ser confiáveis, devem possuir uma arquitetura que permita que os dados permaneçam intactos mesmo que haja falhas ou erros em um ou mais servidores ou máquinas virtuais sobre os quais essas aplicações estão executando.

A *disponibilidade* é uma grande preocupação, pois mesmo sistemas da Google, como o Gmail, já ficaram fora do ar e, por mais que o sistema esteja sempre *on-line*, o usuário sempre necessita do funcionamento da internet, que também é um serviço que não possui disponibilidade em nível de rede local (PEDROSA; NOGUEIRA, 2011, p. 2-4).

Pela forma de funcionamento desses pontos, verifica-se que a própria computação em nuvem já tem, em si, fragilidades que podem comprometer a identificação de pistas de cibercrimes.

A utilização de recursos computacionais deixa pistas (vestígio, indício, evidência, artefato) que podem ser utilizadas para a identificação da materialidade, da dinâmica, da autoria e até da motivação do fato. Entretanto, quando se trata de recursos digitais, há necessidade de uso de técnicas específicas que podem variar de acordo com o caso concreto (NERES, 2021, p. 9).

Pistas tecnológicas são encontradas diuturnamente nas diversas situações do cotidiano das pessoas e das empresas, seja em simples mensagens, seja em consultas bancárias, enfim, na quase totalidade das ações diárias. E a depender da situação, elas podem servir para identificar crimes e sua autoria. Consideram-se pistas “as marcas ou informações em formato virtual, deixadas por usuários em serviços digitais, como arquivos de vídeo e de áudio, documentos de texto, aplicativos de mensagem e de redes sociais” (MACHADO, 2022, p.1), entre outras que a inovação tecnológica venha a disponibilizar em seu processo evolutivo.

1.4 Evidência digital: características, coleta e preservação

Pelo Manual de Patologia Forense (1990) do Colégio de Patologistas Americanos, ciência forense é “a aplicação de princípios das ciências físicas ao direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade”.

Quando se fala em forense, pensa-se logo em crimes e em tentativas de se desvendar quem foi o assassino. Para tanto, dá-se a coleta de objetos, de marcas, de sinais e de outros aspectos relevantes no local do crime, os quais podem se tornar evidências futuras no processo de perícia criminal. Por isso, a depender do material

coletado ou do vestígio encontrado, essa ciência pode atuar em diversos segmentos, como patologia, odontologia, engenharia, biologia, geologia, psiquiatria e também criminalística (PINHEIRO, 2013).

Nesse prisma, a computação forense se insere na ciência criminalística e é definida por como uma disciplina autônoma, integrada pelos diferentes ramos do conhecimento técnico-científico, como meio de auxiliar e informar as atividades policiais e judiciárias de investigação criminal, tendo por objeto o estudo dos vestígios materiais extrínsecos à pessoa física, no que tiver de útil à elucidação e à prova das infrações penais e, ainda, à identificação dos autores respectivos (RABELO,1996 apud MAIA, 2012, p. 7).

Na lição de Pinheiro (2013, p. 280), a computação forense consiste no uso de métodos científicos de preservação, de coleta, de validação, de identificação, de análise, de interpretação, de documentação e de apresentação de evidências digitais, na busca por desvendar objetivamente os elementos: “quem? O quê? Quando? Como? Onde? E por quê?”.

No que diz respeito a “o quê”, os peritos federais Vilar e Gusmão (2016, apud VELHO, 2016, p. 32) salientam que “pistas” digitais nem sempre se encontram confinadas num perímetro bem definido, mas podem estar espalhadas em vários ambientes que precisam ser devidamente tratados pelo profissional especializado encarregado da elucidação desses fatos.

De início, faz-se necessário definir termos técnicos utilizados nesse sentido, visando a eliminar eventuais entendimentos subjetivos que possam interferir no processo científico de coleta e, consequentemente, ocasionar resultados imprecisos ou não verdadeiros. Jesus Antonio Velho (2016, p. 13) faz a seguinte distinção:

- Vestígio: qualquer marca, fato, sinal ou material detectado no local em que se praticou um ato delituoso;
- Indício: circunstância conhecida e comprovada que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias (art. 239 do CPP);
- Evidência digital: toda informação ou assunto criado, sujeito ou não à intervenção humana, que possa ser extraído de um dispositivo eletrônico;
- Artefato: restos de uma atividade de ataque ou de um incidente que pode estar ou não ligado ao invasor.

O que se infere desses termos técnicos e de suas características é que, em dada situação, um deles pode funcionar como requisito para outro (ex.: indício leva a uma evidência ou a artefatos) ou cada um pode ser detectado isoladamente. A evidência digital é objeto deste trabalho.

Na continuidade da referência de Pinheiro (2021, p. 280) aos elementos “como, onde e quando” a serem desvendados, a literatura traz alguns procedimentos. A coleta da evidência digital de maneira mais adequada é substancial na investigação de várias atividades criminosas. Assim, como numa investigação de crime de homicídio em que há um local de crime com indícios e vestígios, deve-se entender o valor de uma evidência bem coletada no local de crime, em tese, virtual (BARRETO, 2016, p.1). É por meio dessa evidência que se pode fundamentar todo o processo de identificação e posterior acusação das pessoas envolvidas no crime.

Desta feita, pode-se inferir que o objetivo da computação forense é estabelecer a dinâmica, a materialidade e a autoria dos ilícitos ocorridos no campo da informática, visando principalmente “a identificação e o processamento de evidências digitais em provas materiais de crime”. Para tanto, utilizam-se metodologias técnico-científicas, “conferindo-lhe validade probatória em juízo” (ELEUTÉRIO; MACHADO, 2011, apud SOUZA, 2023, p. 5).

1.4.1 Evidência digital como prova

No plano abstrato, evidência é uma relação entre certezas na qual uma fortalece a outra, e o conjunto formado por elas valida uma em relação à outra, constituindo uma experiência ou um modo de pensar (ROCKEMBACH, 2013, p. 92).

No plano empírico, o “reino da evidência” se situa entre os fatos e a determinação deles. Na identificação dos fatos, verificando-se afirmações verdadeiras e falsas sobre eles, adentra-se o “reino da evidência”. “Evidência é o que fornece a justificativa ou garantia [...] de que algo é verdadeiro ou falso. [...] são fatos, mas fatos que levam à conclusão sobre se outros fatos existem ou não”. A evidência é pré-requisito de julgamentos da verdade ou da falsidade de algo (SCHAUER, 2022, p. 13).

No plano digital, evidências digitais – oriundas da *common law* com o nome de *digital evidences* – podem ser definidas como “qualquer dado armazenado ou

transmitido por computador, que seja capaz de corroborar ou refutar uma tese sobre a prática de um crime, ou que esclareça elementos determinantes de um crime como a intenção do agente e álibi". São informações que ficam armazenadas ou que foram transmitidas por meio eletrônico sob a forma de *bits* (SOUZA, 2021, p. 31).

Computadores e dispositivos eletrônicos tratam a informação segundo o sistema binário. Esse sistema tem muito de suas bases nos estudos sobre "álgebra *booleana*", no qual símbolos são representados por algarismos que vão de zero a um, sendo essa representação conhecida como digital, por ser embasada em números/dígitos (VAZ, 2012, p. 62).

As definições de evidências ou provas digitais têm vários sentidos ou "correspondem ao sentido de 'elemento de prova'" (VAZ, 2012, p.62). Prado (2021, p.8) argumenta que o surgimento quase cotidiano de novas tecnologias do gênero desanima a elaboração de uma taxonomia das «provas digitais», como aparece, por exemplo, a denominação «ativos de Tecnologia de Informação e Comunicação (TIC)» nos arts. 3º e 4º da Portaria n. 242, de 10 de novembro de 2020, do Conselho Nacional de Justiça (CNJ), que cria o Comitê de Segurança Cibernética do Poder Judiciário brasileiro.

Nesse sentido, o Direito Português se alberga em definições similares – já que se reportam à representação digital, embasada na sequência de números ou dígitos – para se referir ao que constitui uma evidência ou prova digital ou denominação semelhante. Por exemplo: prova eletrônico-digital são informações de todo tipo que contenham valor de prova e que estejam armazenadas em repositórios digitais ou sejam transmitidas por meio de sistemas e de redes de informática, acessíveis de forma privada ou pública e em formato binário/digital (RODRIGUES, 2009, p. 44-46); prova digital é a informação em formato binário, que é transmitida ou que foi memorizada e que pode ser usada pela justiça (International Organization of Computer Evidence); "prova digital são dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias" (VAZ, 2012, p. 62-63).

Pela norma ISO/IEC 27037:201212, evidência digital é informação ou dado que foi armazenado ou transmitido em formato digital ou por meio de suporte informático e que tem valor probatório. Este último elemento – valor probatório – será dado pelas normas processuais de cada país que permitam a utilização das provas recolhidas

num processo judicial, desde que respeitem as diretrizes e os princípios estabelecidos. Nesse sentido: quaisquer dados armazenados ou transmitidos por meio da utilização de computadores (no sentido lato), que apoiem uma teoria sobre como ocorreu um crime ou abordem elementos críticos dele, como a intenção ou o seu álibi. Parece, então, que a prova digital é, em grande parte, associada a qualquer prova que possa ser apreendida num processo judicial (RODRIGO, 2021, p. 140).

As características das evidências digitais são “fatores determinantes” para se cumprirem os procedimentos a serem adotados em sua coleta e demais passos. São elas: imaterialidade, volatilidade e fragilidade (ALMAS; GASTAL, 2021, p. 8), referidas em geral e complementadas: dispersabilidade (SOUZA, 2021, p. 33); necessidade de intermediação para acesso ou indispensabilidade (VAZ, 2012, p. 67).

A imaterialidade é o conceito essencial da evidência digital (ALMAS; GASTAL, 2021, p. 8) e tem relação com suas características não corpóreas, já que ela é constituída de um conjunto de *bits* e de impulsos elétricos; torna a evidência intangível (LEMOS, 2021, p. 19). É, literalmente, a “ausência de representação física” (SOUZA, 2021, p. 33) e diz respeito à impalpabilidade das informações (ALMAS; GASTAL, 2021, p. 8) e à independência do suporte físico no qual se encontra. Entre seus efeitos, a imaterialidade possibilita uma grande capacidade de armazenamento de informações em um dispositivo (porque as informações não ocupam grandes espaços físicos por serem compactadas) e permite um alto nível de transmissibilidade por meio de redes de comunicação (VAZ, 2012, p.67,68). A imaterialidade facilita a clonagem de dados, viabilizando a reprodução de “cópias fiéis aos originais em incontáveis quantidades, ainda possibilitando, em conjunto, a transmissão a distintos dispositivos (KIST, 2019, apud SOUZA, 2021, p. 33).

A volatilidade, relacionada com a imaterialidade, refere-se “ao perecimento da prova digital”. Representa a capacidade de as informações desaparecerem por várias razões, a exemplo de armazenamento em local com temperatura alta, da sobreposição de uma informação sobre outra ou de sua própria natureza temporária, entre outras (ALMAS; GASTAL, 2021, p. 8). Tecnicamente, a volatilidade “se caracteriza pela possibilidade de alteração binária ou algorítmica que poderia inviabilizar o dado digital e, por consequência, a prova digital” (LEMOS, 2021, p. 20). A volatilidade tem relação com a capacidade de mobilidade, com a grande facilidade de sofrer transformações ou modificações, voluntariamente ou não, bastando para

isso, por exemplo, que se altere uma sequência numérica (SOUZA, 2021, p. 33). “A prova digital pode ser alterada ou obliterada maliciosamente pelos infratores ou acidentalmente durante a coleta, sem deixar nenhum sinal óbvio de distorção” (CASEY, 2011, apud LEMOS, 2021, p. 20). Com essa dissipação fácil, o resultado pode ser a perda da informação ou sua adulteração proposital ou acidental durante a coleta, sem deixar nenhum sinal de distorção (VAZ, 2012, p. 69).

A fragilidade se refere ao risco alto de os dados serem contaminados durante algum manuseio (ALMAS; GASTAL, 2021, p. 8). Ela decorre da imaterialidade, qualidade que termina por possibilitar a modificação de dados (VAZ, 2012, p. 68). É por sua fragilidade, entre outras características, que em determinados casos se deve cuidar mais especialmente da preservação de dados, tanto os que se encontram armazenados como os que se encontram do trânsito da comunicação (MENDES, 2020, apud SOUZA, 2021, p. 33).

Dispersabilidade é a capacidade de se expandir e pode ser vista em duas dimensões: viabilidade de coexistência em vários locais dentro do sistema informático em que os dados se encontram inseridos e também em servidores de rede localizados em lugares distintos do mundo (SOUZA, 2021, p. 34).

A indispensabilidade/necessidade de intermediação para o acesso dos dados é decorrente da imaterialidade. Como o dado digital representa uma sequência numérica que constitui um código digital, “faz-se necessário o uso de um equipamento que possa processar a informação e disponibilizá-la de maneira compreensível pelo ser humano. Não é possível a leitura dos dados diretamente pelo receptor da informação, vez que está é imaterial, invisível e codificada” (VAZ, 2012, p. 70, 71).

Por tais características é que as provas digitais têm peculiaridades que as diferenciam de provas materiais. Em processos de transferência das informações digitais, por exemplo, como elas são constituídas de sequências numéricas, cópias são exequíveis. Dessa forma, em caso de transferências para outros dispositivos, é impossível identificar os dados digitais que deram origem às demais. Por isso, “a utilização de métodos indevidos de recolhimento de dados digitais é capaz de comprometer o material, alterando seu estado inicial, proporcionando sua deterioração” (ALMAS; GASTAL, 2021, p. 9).

Em outra perspectiva, de modo geral, a validade de uma evidência digital fundamenta-se em três pilares: relevância – toda evidência digital é relevante se for destinada a comprovar ou a descartar elementos de determinado caso sob investigação; confiabilidade – qualidade que assegura que a evidência é aquilo que "que pretende ser"; suficiência – que encontra o bastante para poder examinar adequadamente os elementos questionados/investigados (OLIVEIRA, 2023, p. 5).

A respeito da prova em si, de início, considera-se que sua definição depende da área do conhecimento enfocado. Prova pode significar: os instrumentos utilizados pelo magistrado para conhecimento dos fatos em análise, por meio do material definido em lei; o procedimento pelo qual a cognição é organizada e se forma, sendo apresentada ao juízo; a "atividade lógica para o juiz, para a percepção dos fatos" – como epistemologia, indução, dedução, percepção – e ainda, o resultado da lógica do juízo que tende ou não à busca da "verdade dos fatos", como defendem Taruffo (2002) e Liebman (1984) (apud BERBERI; HANTHORNE, 2021, p. 142).

Na prática nessa temática, visando estabelecer uma hierarquia de provas, a justiça brasileira norteia-se pelos seguintes princípios: *admissibilidade* – condições de a prova ser usada no processo; *autenticidade* – uma prova certa e de relevância para o caso concreto; *completude* – capacidade de a prova convalidar as suspeitas apresentadas; *confiabilidade* – não deve haver dúvidas quanto à veracidade e à autenticidade da prova; *credibilidade* – refere-se à clareza e à interpretação humana da prova coletada (PINHEIRO, 2021, p. 281).

Na perspectiva teórica da prova, evidência digital ou prova digital é o "instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para a sua demonstração". Evidência/prova digital é um meio de se comprovar tanto um ato realizado em meio digital como um ato no qual o meio digital tenha um instrumento digital como forma de demonstrar o conteúdo desse fato (THAMAY; TAMER, 2020, apud BERBERI; HANTHORNE, 2021, p. 147).

Assim, associando as características teóricas da prova às particularidades dos dados digitais, no sentido amplo, pode-se resumir: prova digital não é nada mais nada menos que todo e qualquer dado que esteja armazenado ou que seja transmitido via computador e sirva para apoiar ou para rejeitar alguma teoria sobre como um crime

específico aconteceu e que contenha elementos críticos desse crime, como intenção ou álibi. A prova digital é “assimilada a qualquer prova que possa ser apreendida num processo judicial” (RODRIGO, 2021, p. 140).

Com frequência, opositores questionam se o embasamento de alguma conclusão jurídica se deu em “evidências sólidas”, “evidências concretas”, “evidências conclusivas” ou “evidências definitivas”. Da mesma forma, se as objeções são justificadas como falhas de “prova”, afirmam que a prova é mais forte que a evidência e que nenhuma evidência pode alcançar o nível de prova. À alegação de que há falta de “evidências conclusivas ou definitivas” para uma conclusão indica que existe alguma evidência apoiando a conclusão. Já a alegação de evidências não suficientemente conclusivas, persuasivas, definitivas, sólidas ou concretas significa que pode ser necessário um ônus de prova mais específico (SCHAUER, 2022, p. 53-57). Esses questionamentos, contudo, não são específicos das evidências/provas digitais, mas de qualquer tipo de prova. Em relação às evidências digitais, eles podem estar relacionados com os pilares de sua validade, anteriormente citados por Oliveira (2023), especificamente a suficiência.

O uso de evidências digitais, sem questionamentos sobre sua validade ou sobre seu valor probatório, requer que elas estejam em conformidade com, pelo menos, dois princípios: autenticidade – propriedade essencial, asseguradora de que os fatos ali dispostos estão de acordo com o fato jurídico ocorrido e que foram praticados pelos seus respectivos autores; integridade – garantia de que a evidência não sofreu qualquer adulteração desde sua coleta (THAMAY; TAMER, 2020, p. 40).

Diante disso, entre outras condições, ratifica-se a importância da presença de especialistas que detenham densos conhecimentos nas áreas de Direito Digital e perícia forense digital em casos dessa natureza, com vistas a evitar a contaminação ou a anulação da prova coletada.

1.4.2 Meios e procedimentos para coleta e preservação de evidências digitais

Em razão da amplitude de um crime cibernético, que pode englobar uma extensa série de transgressões, somada ao elevado grau de complexidade técnica comumente envolvida na identificação de sua origem, a justiça brasileira tem-se

utilizado de profissional especializado (perito) para nortear as partes e o juiz na interpretação e nas comprovações técnicas das evidências digitais acostadas no caso concreto. Apesar de a computação prover um elevado quantitativo de evidências digitais, há necessidade de utilização de técnicas específicas, que demandam conhecimento especializado, de forma a garantir o cumprimento da hierarquia de provas já mencionada.

Nesse sentido, um dos norteadores da ciência forense moderna é conhecido como “Princípio da Troca de Locard”, desenvolvido pelo cientista forense francês Edmond Locard. Segundo ele, qualquer um ou qualquer coisa que entra em um local de crime leva consigo algo do local e deixa alguma coisa para trás quando parte. Apesar de esse princípio ter sido proposto para vestígios físicos aplicados a cenas do crime (como pegadas e sangue), seu emprego em casos de vestígios digitais também é amplamente aplicado. Nesse caso, considera-se a necessidade de ponderações relativas às alterações no plano físico (*hardware*) e lógico computacional (*software*). Elas perduram nas cinco macroetapas da perícia forense digital, quais sejam: identificação, isolamento, registro, coleta e preservação (SOUZA *et al*., 2023, p. 57-61).

No âmbito digital, a simples coleta de evidências sem utilização de técnica adequada pode eliminar todas as chances do litígio judicial, devido à contaminação do local do crime. Da mesma forma, ocorre com a coleta sem o emprego de manutenção e de registro histórico cronológico das evidências (cadeia de custódia), haja vista a possibilidade de a parte contrária argumentar sobre as evidências terem sofrido adulterações durante seu manuseio (THAMAY; TAMER, 2020, p. 161).

Segundo a citada norma ISO/IEC 27027/2013, os principais procedimentos para identificação, coleta e aquisição da evidência digital são: “cadeia de custódia, precauções no local do incidente, papéis e responsabilidades, competência, utilização de cuidado razoável, documentação, instruções, priorização da coleta e aquisição e preservação da potencial evidência digital”. Com eles, a solução tecnológica estará plenamente atendida (PASTORE; FONSECA, 2022, p. 107).

Ante a fragilidade da evidência digital, o tratamento para assegurar sua integridade e autenticidade deve ser padronizado. E os principais elementos que possibilitam a credibilidade da investigação são: qualificação das pessoas para execução das tarefas e aplicação de metodologia adequada. O primeiro se refere a

interventores – pessoas com conhecimento suficiente para auxílio no manuseio de evidência digital – e a especialistas – indivíduos com grande experiência e condição de assegurar sua preservação; o segundo, à norma que padroniza o tratamento de evidências digitais em todas as etapas do processo (OLIVEIRA, 2023, p. 6).

1.4.3 A cadeia de custódia

No ambiente virtual (ciberespaço), surge um novo problema, diretamente relacionado com o Direito: como obter e manter íntegras as evidências digitais oriundas de ambientes em nuvem com grande massa de dados?

O Pacote Anticrime, Lei n. 13.964, de 2019, dispõe sobre a cadeia de custódia dos vestígios e se divide em várias etapas: identificação, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte (PASTORE; FONSECA, 2022, p. 98). O objetivo desse conjunto de procedimentos a serem utilizados é a manutenção e a documentação da cronologia do vestígio criminoso, como possibilidade de rastrear sua posse e manuseio, bem como seu curso seguinte até o descarte (MPPR, 2016, p. 290).

No entanto, o legislador só descreveu a cadeia de custódia de provas físicas e materiais de forma detalhada, e não tratou dos procedimentos referentes à custódia de evidências digitais, as quais são mais frequentes, devido à crescente ocorrência de cibercrimes (PASTORE; FONSECA, 2022, p.98).

A evidência digital colocou o processo penal diante de um problema jurídico em relação à possível adaptação dos meios tradicionais de prova às novas tecnologias e também confronta o processo penal com a formulação de novos meios de prova, coerção probatória ou medidas investigativas, comumente abrangidos pela denominação de meios de prova simplesmente pelo capítulo da lei que os estabelece – (por exemplo, acesso transfronteiriço a dados, acesso remoto ou uso de *software* malicioso pelo Estado). Numa ou noutra tarefa, o exame jurídico é complexo e exige discussões aprofundadas sempre atravessadas pela proteção das garantias constitucionais (principalmente, o direito à privacidade) e pela garantia da certeza do elemento probatório (cadeia de custódia). O progresso tecnológico exige o acompanhamento do direito penal e das garantias, por meio de uma revisão

abrangente de tais conceitos, que devem ser adaptados a este novo paradigma social, para proporcionar uma proteção eficaz e uma resposta satisfatória (RODRIGO, 2021, p. 140).

Essa é uma lacuna que precisa ser suprida devido a possíveis prejuízos processuais que possam ocorrer, como inadmissibilidade ou exclusão de provas digitais dos autos ou até redução da força probatória, conforme o entendimento seguido (PASTORE; FONSECA, 2022, p.98).

De forma ampla, a cadeia de custódia é conceituada como a reunião de procedimentos que visam a documentar a origem, a identificação, a coleta, a custódia em si, o controle, a transferência, a análise e o destino das evidências digitais (PARODI, 2020, p. 1). Também como um mecanismo que visa a assegurar a autenticidade das evidências digitais coletadas e o respectivo exame, garantindo tratar-se do material correspondente ao crime sob investigação, sem nenhuma margem de espaço para eventuais adulterações. Em resumo, tem-se que a documentação formal dos procedimentos realizados para manter e registrar a cronologia das evidências digitais, e sua preservação, contra interferências externas e mesmo internas, possibilita seu rastreamento do local do crime até o juízo, salvaguardando-as de dúvidas na atividade probatória e assegura (PASTORE; FONSECA, 2022, p. 99).

Em outros conceitos, a cadeia de custódia: equivale a um conjunto de pessoas que “tiveram contato com a fonte de prova real” de forma sucessiva, e à documentação relativa à formalidade referente a essas pessoas (quem) e aos “momentos em que mantiveram o contato (quando)”. Ainda: “a cadeia de custódia corresponde à atividade probatória secundária, ou seja, a ‘prova sobre a coleta da prova’, ou, mais sinteticamente, ‘a prova da prova’. Ou, ainda, ‘uma prova de segundo grau ou meta prova’”, explicam Pastore e Fonseca (2022, p. 99).

No processo penal, a noção de preservação da cadeia de custódia se refere à segurança da integridade da evidência digital e, consequentemente, da credibilidade e de sua prestabilidade como prova. Presta-se também ao pleno exercício do contraditório; as partes devem ter acesso a provas íntegras, embora o destinatário delas seja o juiz (PARODI, 2020, p. 1).

A cadeia de custódia começa com a preservação do lugar onde aconteceu o

crime e/ou com os procedimentos periciais ou policiais referentes à detecção da evidência. De forma breve, os procedimentos da cadeia de custódia são assim descritos (MPPR, 2016, p. 290):

- reconhecimento: ato de distinguir elementos de interesse potencial à produção da prova pericial;

- fixação: descrição do vestígio com detalhes, como foi encontrado no lugar do crime e respectiva posição na área examinada por meio de ilustrações;

- coleta: recolhimento do vestígio a ser submetido à perícia, respeitando-se a respectiva natureza e suas características;

- acondicionamento: embalagem individual dos vestígios coletados, de acordo com as características físicas, biológicas e químicas, anotando-se todos os dados cronológicos, inclusive hora e identificação do profissional responsável pela coleta e pelo acondicionamento;

- transporte: transferência do vestígio de um local para outro, dentro das condições e meios adequados ao tipo de evidência, visando à garantia de manutenção de suas características originais e do controle de sua posse;

- recebimento: formalidade referente à transferência da posse do vestígio, com documentação contendo, pelo menos, as informações: “número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome do transportador, código de rastreamento, natureza do exame, tipo do vestígio, protocolo e assinatura/identificação de quem recebeu”;

- processamento: exame pericial propriamente, devendo o vestígio ser manipulado com base em uma metodologia que se adeque a todas as suas características, para que o resultado buscado possa ser formalizado por meio de um laudo;

- armazenamento: guarda do material a ser submetido a processamento na realização de contraperícia, transportado ou descartado com a devida vinculação ao respectivo número do laudo;

- descarte: “procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial” (MPPR, 2016, p. 290-291).

“A violação da cadeia de custódia implica a impossibilidade de valoração da prova, configurando seu exame – de verificação da cadeia de custódia – um dos objetos do juízo de admissibilidade do meio de prova ou do meio de obtenção de prova”. As consequências do não atendimento a essa cadeia (quebra da cadeia) não são submetidas a nenhum juízo de peso probatório, nem à relevância da prova. Essa condição também é válida no caso das provas digitais. Didaticamente falando, da mesma forma que o problema requer revisitar “o papel do corpo de delito na apuração da responsabilidade criminal”, no caso da prova digital, exige que se verifiquem suas especificidades tecnológicas (PRADO, 2021, p. 1-2).

O Pacote Anticrime (Lei n. 13.964/2019) não prevê de forma expressa consequências jurídicas para a não observância de qualquer etapa da cadeia de custódia. Com isso, houve um dissenso doutrinário importante, com dois posicionamentos básicos: a quebra da cadeia de custódia acarreta ilicitude e leva à inadmissibilidade/exclusão dos vestígios dos autos e das decorrentes provas; “o rompimento da cadeia de custódia não afeta a admissibilidade e validade processual, mas a sua valoração probatória, isto é, o seu peso na formação de convencimento do julgador” (PASTORE; FONSECA, 2022, p.101).

Sobre as evidências digitais, duas fontes normativas podem ser citadas, com padrões a elas aplicáveis: a referida NBR ISO/IEC n. 27027/2013, da Associação Brasileira de Normas Técnicas (ABNT), e a RFC 3227/2002, da International Engineering Task Force (IETF) (PASTORE; FONSECA, 2022, p.101-102).

A aplicação da NBR ISO/IEC 27037/2013 está de acordo com leis, regulamentos e regramentos internacionais, mas ela não deve substituir nenhuma exigência legal de qualquer jurisdição, e sim direcionar a prática de interventores e especialistas em investigações que envolvam evidências digitais em potencial (OLIVEIRA, 2023, p. 6).

1.5 Desafios das provas digitais na computação em nuvem

Nos últimos anos, a computação em nuvem tornou-se cada vez mais popular, à medida que mais e mais organizações movem seus dados e aplicativos para esse ambiente de recursos e de provisão de serviços computacionais. A computação em

nuvem oferece muitos benefícios, incluindo escalabilidade, flexibilidade e economia, mas também apresenta novos desafios em termos de perícia digital, como já dito.

O ambiente de nuvem representa a convergência de campos de tecnologia, como: "*hardware,* com capacidade de virtualização; tecnologias de Internet" (Web 2.0 e serviços web); gerenciamento de sistemas (computação independente, automação de gerenciamento e manutenção de *data center*) e computação distribuída, em especial, a *utility & grid computing* (PEDROSA; NOGUEIRA, 2011, p. 2) ou o fornecimento de serviços e recursos de computação a clientes e combinação de recursos de vários domínios administrativos para alcançar um objetivo comum.

Outro ponto importante para o entendimento deste modelo de computação refere-se aos participantes da nuvem, que podem ser divididos em três grandes grupos: Provedor de Serviço, Desenvolvedor e Usuário. O provedor é responsável pela tarefa de disponibilizar, gerenciar e monitorar toda a infraestrutura da nuvem, garantindo o nível do serviço e a segurança adequada de dados e aplicações. Já o desenvolvedor deve ser capaz de prover serviços para o usuário final, a partir da infraestrutura disponibilizada pelo provedor de serviço, enquanto o usuário final é o consumidor que irá utilizar os recursos oferecidos pela nuvem computacional (SILVA, 2010, apud PEDROSA; NOGUEIRA, 2011, p. 1).

Essa descrição dos participantes já possibilita dimensionar, teoricamente, as dificuldades de obtenção de dados inseridos na computação em nuvem, principalmente se se considerar que o provedor e o desenvolvedor estão distantes dos milhões de usuários, ou seja, não se sentem afetados diretamente com o que pode acontecer a eles. Acrescente-se a isso o fato de não haver, como já explicado, um ponto central (*hub*) que concentra a totalidade dos dados. A dispersão dos dados entre servidores retarda a busca.

Os provedores dos serviços em nuvem garantem confiabilidade e segurança dos dados, mas, mesmo assim, ataques concretizados nesse ambiente são muito difíceis de ser investigados e trazem muitos desafios para os peritos digitais forenses. As dificuldades vão desde a forma de coletar as evidências digitais, muitas vezes distribuídas em locais geograficamente diferentes, passando pelo acesso a informações que podem se encontrar sob responsabilidade de um provedor, até questões legais (SOUZA, 2023, p. 1-2).

É nesse contexto que a análise forense em nuvem – processo de coleta, análise e preservação de evidências digitais de sistemas e aplicativos baseados em nuvem – se realiza. O processo envolve a utilização de técnicas forenses tradicionais no ambiente de nuvem, bem como o desenvolvimento de novos métodos e ferramentas para enfrentar os desafios exclusivos impostos por esse ambiente. (SOUZA *et al*., 2023, p. 57)

Ruan *et al*. (2011 apud SOUZA, 2023, p. 7) categorizaram os desafios na análise forense em computação em nuvem em três dimensões: técnica, organizacional e jurídica. A dimensão técnica se refere ao processo de coleta dos dados, à "elasticidade das ferramentas de forense *in live*, divisão das informações que podem estar compartilhadas em locais diferentes e os requisitos contratuais"; a organizacional diz respeito às responsabilidades dos provedores e dos usuários; a jurídica se volta para as questões legais e para os Service Level Agreements. Cada uma dessas dimensões contém "fatores que definem as ferramentas, métodos, funções e responsabilidades de cada papel na *cloud forensics*", que definem como como a aplicação da ciência forense digital em ambientes de computação em nuvem, pode ser utilizada.

Ruan *et al*. (2011 apud SOUZA, 2023, p. 7) explicam que os desafios da análise forense em nuvem têm relação com as seguintes situações: jurisdição dos locais onde os dados se encontram armazenados e falta de colaboração internacional para acesso a eles, quando estão em outros países; falta de legislação e regulamentação, que dificulta a recuperação de evidências, principalmente no caso de evidências confidenciais; dificuldade de alcançar a cadeia de dependência entre provedores na nuvem, principalmente devido à terceirização de serviços; indefinição de cláusulas contratuais com os provedores no sentido de disponibilizar as informações solicitadas, necessárias à investigação; grande aumento de dispositivos com acesso à nuvem; "divisão dos dados forenses em uma infraestrutura que é compartilhada por diversos usuários".

A propósito, o National Institute of Standards and Techonology (NIST) lista vários desafios que os profissionais forenses enfrentam em investigações realizadas em nuvem de computação por conta de crimes cibernéticos, como os citados a seguir.

Os peritos forenses têm dificuldades em identificar a autoria e em atribuir responsabilidade pela exclusão de dados em nuvem devido ao grande número de

usuários e ao volume de dados que compartilham o serviço, o que dificulta aos provedores em nuvem implementarem métodos de *back-up* que possa recuperar essas informações. A reconstrução de armazenamento virtual em ambientes de nuvem a partir da cópia do disco físico também se torna bastante complexa, pois os algoritmos de reconstrução precisam ser validados ou muitas vezes desenvolvidos. A preservação das evidências pode ser prejudicada devido à falta de conhecimento da arquitetura utilizada, sincronização entre os servidores, códigos maliciosos, erros de no gerenciamento ou configurações de serviços em nuvem realizados de maneira incorreta (NIST, 2014, apud SOUZA, 2023, p. 7-8).

Como se pode ver, se o processo penal ainda não tem resolvidas todas as questões referentes a crimes cibernéticos realizados em ambientes locais, no ambiente de computação em nuvem, as dificuldades são elevadas a um patamar sem estimativa. Isso porque, além das características peculiares das evidências digitais, marcadas pela imaterialidade e tudo o que ela acarreta ou proporciona, elas envolvem questões outras, que implicam acordos entre países.

2 PROVAS DIGITAIS E COMPUTAÇÃO EM NUVEM NO DIREITO BRASILEIRO FRENTE AO DIREITO COMPARADO

No atual cenário nacional, a legislação restringe-se à custódia de provas eletrônicas físicas (discos rígidos, *smartphones, tablets* etc.), o que implica novos desafios dentro da computação em nuvem, uma vez que os elementos não são mais unitários, mas sim distribuídos em vários ativos de Tecnologia da Informação e comumente inacessíveis a um perito.

Restos ou vestígios podem constituir provas digitais e, portanto, como qualquer prova, no ambiente do crime, cautela e muito cuidado são procedimentos necessários quando de sua apreensão, a qual deve ser realizada conforme as indicações das fases que integram a cadeia de custódia, prevista no CPP. Pelo art. 158-A desse Código, cadeia de custódia é “o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte” (MACHADO, 2022, p. 1).

Verificando o art.158-B, os citados procedimentos são definidos por uma ação que compreende as etapas e os respectivos tratamentos:

> Art. 158-b. a cadeia de custódia compreende o rastreamento do vestígio nas seguintes etapas: (incluído pela lei n. 13.964, de 2019) (vigência)
> I - reconhecimento: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial; (incluído pela lei n. 13.964, de 2019) (vigência)
> II - isolamento: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime; (incluído pela lei n. 13.964, de 2019) (vigência)
> III - fixação: descrição detalhada do vestígio conforme se encontra no local de crime [...] e a sua posição [...], sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento; (incluído pela lei n. 13.964, de 2019) (vigência)
> IV - coleta: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza; (incluído pela lei n. 13.964, de 2019) (vigência)

> V - acondicionamento: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento; (incluído pela lei n. 13.964, de 2019) (vigência)
> VI - transporte: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse; (incluído pela lei n. 13.964, de 2019) (vigência)
> VII - recebimento: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu; (incluído pela lei n. 13.964, de 2019) (vigência)
> VIII - processamento: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito; (incluído pela lei n. 13.964, de 2019) (vigência)
> IX - armazenamento: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente; (incluído pela lei n. 13.964, de 2019) (vigência)
> X - descarte: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial. (incluído pela lei n. 13.964, de 2019) (vigência).
> O Art. 158-C estabelece que a coleta de vestígios deve ser preferencialmente realizada por perito oficial, responsável que vai dar o encaminhamento devido à central de custódia.

Trazendo o estabelecido no artigo acima para o campo das evidências digitais, de início, é importante alocar a evidência como espécie pertencente ao gênero prova científica. Isso significa que, para uma coleta bem-sucedida, bem como para manipulação e tratamento de tais vestígios, a operação deve ser guiada por critérios e métodos científicos e, por consequência, requer habilidade e competência do responsável, ou seja, pessoa dotada de qualificação e *expertise* para tanto.

Destaque-se nesse sentido que “a definição embasada e criteriosa de uma ciência valorativa das provas” não deve ser confundida com procedimentos acríticos

relativos aos elementos de prova de cunho científico. Deve sempre haver e prevalecer o convencimento livre motivado em conjunto com outros meios de se provar (SOUZA, 2021, p. 31).

A primeira regulamentação de uma inovação tecnológica se deu por meio da Lei n. 9.800/1999, que dispôs sobre a possibilidade de se apresentar documentos e de até interpor recursos por meio de *fac-símile*. Contudo, mesmo utilizando esse meio, as partes se obrigavam a apresentar os documentos físicos depois. Obviamente, não se tratava de uma prova digital em si, mas de "documentos que se prestam à transmissão de informações por meio de redes de comunicações" (MARINONI *et al*., 2015, apud BERBERI; HANTHORNE, 2021, p. 144). Era uma forma de antecipar a documentação e, de certo modo, agilizar o processo.

Os arts. 212 e 225 do Código Civil de 2002 dispõem sobre a utilização de meios eletrônicos e sobre a reprodução de coisas ou de fatos como forma de prova. Em 2006, a Lei n. 11.419 estabeleceu a informatização do processo judicial, representando "um marco regulatório essencial para a informatização do Judiciário brasileiro". Depois, a Resolução n. 185 de 2013, do Conselho Nacional de Justiça, instituiu o Sistema de Processo Judicial Eletrônico para processar as informações e as práticas dos atos processuais, distinguindo, então, em seu art. 3º, "documento eletrônico" de "processo eletrônico". Ainda que timidamente, o CPC, em 2015, nos arts. 422, § 1º, 439, 440 e 441, dispôs sobre a prova eletrônica como documento eletrônico (BERBERI; HANTHORNE, 2021, p. 144-145).

Todavia, a leitura do art. 439 do CPC/2015 sugere que o legislador considera o suporte físico em papel como regra geral. O artigo dispõe: "A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e da verificação de sua autenticidade, na forma da lei". O CPC não inovou, como indicam suas raízes nos processos físicos, bem afastadas da atual realidade da maioria dos processos em meios eletrônicos (BERBERI; HANTHORNE, 2021, p. 145). Além disso, a expressão "processo convencional" sugere que "os autos do processo não sejam, eles próprios, eletrônicos" (ZAMIDI, 2019, p. 4).

Embora o legislador tenha abordado, de certo modo, o valor da prova na forma digital, a análise do valor probatório é de competência do juiz, em cumprimento ao princípio do convencimento motivado e livre, segundo o art. 371 e disposição do art. 440 do mesmo CPC/2015. Tal posicionamento do legislador suscitou críticas no

âmbito acadêmico em geral, a exemplo do que explicitam Luiz Guilherme Marinoni e Sergio Cruz Arenhart (2019, apud BERBERI; HANTHORNE, 2021, p.145):

> [...] se o documento não for convertido ao meio físico pode o juiz dar-lhe o valor que entender adequado, desde que assegure às partes do processo o seu teor (art. 440 do CPC/15). Novamente, um preceito sem qualquer valor. Afinal, sempre cabe ao juiz avaliação do valor probante de todas as provas, sendo também inquestionável que as partes devem ter direito de acessar as fontes de prova realizadas, até para que possam exercer o contraditório.

Já o art. 441 desse CPC ratifica, de certa forma, a sugerida preocupação do legislador quanto a provas digitais. Reza o referido artigo: “Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica”, levando ao questionamento, entre outros, dos seguintes pontos: há diferença entre prova originalmente digital e prova elaborada por meio eletrônico? O que se considera como prova digital e qual a respectiva natureza jurídica? Respostas para essas perguntas podem ser encontradas em dois campos específicos: na finalidade da prova e no sentido da palavra “digital”, associado ao termo “prova” (BERBERI; HANTHORNE, 2021, p. 146).

No que tange à finalidade/objetivo, se no sentido geral a prova visa convencer o juiz sobre a ocorrência de um fato ou de um direito, e esse magistrado vai exercer seu convencimento livre, motivado por essa comprovação, não há nenhuma diferença entre provas físicas e provas digitais, posto que ambas têm a mesma finalidade essencial. Elas vão se distinguir apenas quanto ao suporte, pois enquanto a prova física se encontra em papéis ou objetos corpóreos, por exemplo, “a prova eletrônica é constituída” por um conjunto de *bits*, ou seja, apenas ‘uma unidade de informação’”. Em resumo, nem o conceito nem o objetivo nem o objeto de prova mudam, apenas seu suporte (RAFFUL; RAFFUL, 2017, p. 64).

No entanto, quanto ao termo “digital” especificamente, o sentido pode variar. A prova digital pode se referir tanto a um fato que tenha se dado no meio digital, ou seja, o suporte do fato tenha sido o meio digital (WhatsApp, Instagram), quanto a uma prova que, apesar de não ter uma origem digital propriamente dita, “a demonstração de sua ocorrência se dá por meios digitais”, por exemplo, fotografias em mídias sociais para demonstrar algo (BERBERI; HANTHORNE, 2021, p. 146). Infere-se daí que, semanticamente, o termo “digital” pode ser entendido como fim e como meio.

Como exemplo, podem ser citadas as provas digitais entregues à justiça por conta da operação “Câmbio, Desligo”. De acordo com o Ministério Público Federal (MPF), os criminosos eram auxiliados por “uma rede de doleiros”, que compensava as transações e “lavava” dinheiro para várias organizações criminosas. Para tanto, as provas apresentadas eram de sistemas próprios de informatização, chamados *Bankdrop* e ST. Nesses sistemas, a perícia da Polícia Federal não identificou a cadeia de custódia digital, finalizando com a informação: “inconclusivo para tempo, data e valores”. A veracidade das informações encontradas no sistema não pôde ser comprovada (MACHADO, 2022, p. 3).

Sobre a temática da prova digital, mesmo em ativos digitais físicos, a jurisprudência do Superior Tribunal de Justiça (STJ) distinguia a prova digital de seu conteúdo. Demandava autorização judicial específica e justificada ou consentimento livre do próprio usuário para verificação de dados constantes em aparelho celular, para acesso a provas digitais decorrentes de acessos a Short Message Service (SMS), de conversas por meio de programa ou aplicativos e de mensagens enviadas ou recebidas por correio eletrônico, sob pena de inadmissibilidade desses dados como prova (prova ilícita), tal como ocorreu em operações de ampla repercussão, como a operação Satiagraha*,* de 2015 (ANULAÇÃO..., 2015), e a operação Spoofing, de 2019, conduzidas pela Polícia Federal do Brasil.

No acórdão vinculado a RCL n. 36734/SP (2018/0285479-8), de 22.02.2021, a 3ª Turma do STJ alterou esse posicionamento, entendendo que, apesar de o acesso a mensagens do WhatsApp sem autorização judicial violar uma garantia fundamental, poderia ser feita a repetição do ato processual viciado, dessa vez com autorização judicial, numa tentativa de tornar válidas as provas inicialmente classificadas como ilícitas.

No âmbito do Supremo Tribunal Federal, no HC 222.141, de 1º de dezembro de 2022, o ministro Ricardo Lewandowski anulou provas colhidas pelo Ministério Público do Paraná na Operação Taxa Alta, deflagrada em 2020. Essa operação apurou a manipulação no processo de credenciamento das empresas para registro de financiamento no Departamento Estadual de Trânsito do Paraná, sob o argumento de indisponibilidade de acesso aos registros de que trata a Lei 12.965/2014 – que “estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (dados intercambiados)” –, o qual deverá ser precedido de indispensável autorização

judicial, independentemente de se tratar do Ministério Público e de autoridades policiais/administrativas, em atenção à referida cláusula constitucional.

Na prática, com a decisão, as provas obtidas dos provedores de Internet a pedido do MP/PR se tornaram nulas. O *parquet* havia solicitado o congelamento do conteúdo da conta dos investigados armazenado em nuvem (*e-mails*, mensagens, contatos e históricos de localização) sem autorização judicial. Diante disso, em sua decisão, o ministro citou a violação à Constituição e ao Marco Civil da Internet, lembrando que o pedido de indisponibilidade dos registros "deverá, a toda evidência, ser precedido de indispensável autorização judicial":

> • Os exemplos mencionados ratificam a necessidade de regulação dessa temática, para mitigar riscos e para gerar segurança jurídica. A repetição de prova oriunda de ambiente digital em momento posterior pode ser prejudicada pela volatilidade das evidências digitais e comprometer sua integridade ou preservação.

2.1 Legislação brasileira: perspectivas

No cenário **brasileiro**, importantes avanços ocorreram nos últimos anos, como a promulgação do Marco Civil da Internet (MCI), em 2014. O MCI inovou no regramento de registro de auditorias de provedores de conexões e aplicações (arts. 10 a 17) e exige que empresas que desejam atuar com o público brasileiro tenham sede em território nacional. *In verbis*:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses **atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira** e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º **O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil**.

> § 3º Os provedores de conexão e de aplicações de Internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. (grifos nossos)

Posteriormente, a Lei n. 13709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) –, objeto da Medida Provisória n. 869, de 27 de dezembro de 2018, dispôs sobre a proteção de dados pessoais e alterou o texto da Lei n. 12.965/2014, chamada de Marco Civil da Internet. A LGPD foi embasada no General Data Protection Regulation (GDPR) europeu – a Regulamentação Geral de Proteção de Dados –, revisando o processamento e o tratamento de dados pelas empresas. O Brasil, de certa forma, ficou equiparado às regras fortes mundiais de proteção de dados. O GDPR, acordo mútuo, entrou em vigor no Brasil em agosto de 2020, a fim de projetar-se na modernização de leis de proteção a informações pessoais (FERNANDES *et al*., 2020, p. 8).

A Lei Geral de Proteção de Dados Pessoais brasileira, que entra em vigor agora, possui semelhanças com o GDPR. Inclusive, não é difícil perceber que muitos artigos da LGPD possuem clara inspiração na lei europeia. Por exemplo, no N. Recurso Especial n. 1.348.532/SP, de outubro de 2017, o Ministro Luiz Felipe Salomão, numa breve análise de Direito Comparado, faz referência direta ao Regulamento europeu e destaca que o conteúdo do art. 5º do GDPR “consagra, entre os princípios fundamentais relativos aos dados pessoais, que a recolha dos dados somente poderá existir com fins específicos, além de estabelecer a minimização dos dados (apenas aquilo que for estritamente necessário), sempre para um fim concreto, além de estabelecer que referido processo seja transparente, leal e lícito” (KING, 2020, p. 6).

Fernandes *et al*. (2020, p. 11) analisaram os impactos da LGPD e concluíram que a legislação brasileira sobre a proteção de dados tem impactos sobre a computação em nuvem. É que a legislação antes vigente não era abrangente, já que dava aos Estados o poder de implementarem padrões mínimos. Com isso, os padrões de proteção de dados adotados eram inadequados e geravam incertezas quanto à opção pela tecnologia em nuvem. Na atualidade, a LGPD, tanto quanto o GDPR, “é abrangente e os provedores de nuvem precisam alterar e modificar seus serviços, processos e contratos para atender aos requisitos da legislação”.

Essa abordagem, embora com foco diferente de investigação, tem relação com o tema deste trabalho, porque demonstra lacunas legislativas que já poderiam interferir desde a opção pela computação em nuvem. Já se indicava aí a necessidade de revisão de processos e de contratos com provedores. Inclusive, sobre esse último item, vale lembrar que questões relacionadas ao nível dos contratos foram apontadas por Ruan *et al*. (2011, apud SOUZA, 2023, p. 7) como um dos desafios da dimensão jurídica enfrentados pelos peritos na análise forense em computação em nuvem.

Depois, veio a creditação da Convenção de Budapeste pelo Brasil, em 17 de dezembro de 2021. Em suas "Disposições Específicas – Auxilio mútuo em matéria de medidas provisórias, o art. 29 – Conservação expedita de dados informáticos armazenados" – dispõe sobre as solicitações de conservação de dados informáticos armazenados, estabelecendo que "a Parte requerente solicite à requerida a manutenção de determinados dados informáticos, uma vez que a Parte requisitante prevê solicitar um pedido de auxílio mútuo de busca, acesso, apreensão, ou obtenção por meio similar ou divulgação sobre tais dados". Todavia, Fonseca e Gennarini (2022, p. 11) explicam que tal dispositivo tem implicações diretas sobre o art. 13 do MCI, de 2014, que reza o seguinte:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> [...]
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.

Em sua análise, Fonseca e Gennarini (2022, p. 11) avaliam que, se uma determinada parte fizer uma solicitação ao Brasil de dados informáticos registrados em provedores de conexão à Internet localizados no território brasileiro, e os dados solicitados se referirem a um ano ou mais de registro, o pedido pode não ser atendido, porque o prazo de armazenamento estabelecido pelo MCI é de um ano, não mais.

Esses autores também argumentam o seguinte: ainda que o § 2º do artigo 13 refira que o Ministério Público ou a autoridade policial ou administrativa pode "requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no *caput* [...]", um ano, o requerimento teria de ser feito antes desse prazo.

Portanto, na hipótese, a assistência mútua solicitada pela parte requisitante deveria ser feita a tempo de o requerimento ser direcionado ao provedor antes de vencer o lapso temporal estabelecido. Isso, mesmo se tratando apenas de conservação/ manutenção dos dados (FONSECA; GENNARINI, 2022, p. 11).

Por seu turno, ainda na perspectiva de solicitações feitas por alguma parte, sob os auspícios do art. 29 da Convenção de Budapeste, o art. 11 do MCI reza o seguinte:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, **deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos** à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Com esses exemplos referentes ao MCI e à LGPD, fica claro que há questões internas a serem resolvidas no cenário jurídico brasileiro, a fim de se evitarem barreiras ou dificuldades ao andamento da persecução penal de crimes cibernéticos.

Além dessas lacunas, no que diz respeito à definição de uma autoridade central para concentrar esse tipo de tratativa em matéria penal, atualmente, o entendimento pacificado é no sentido de que, exceto nos pedidos de MLAT para o Canadá, que são centralizados pela Procuradoria-Geral da República, os demais são de competência do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça e Segurança Pública (MJ, 2023, p. 1).

Segundo determinação do Ministério, todos os órgãos de investigação ou autoridades policiais competentes têm prerrogativa para encaminhar pedidos de cooperação jurídica internacional em matéria penal, seja em âmbito federal ou estadual: Ministério Público Federal, Ministério Público Estadual, Delegacias Federais e/ou Estaduais de Polícia, Juízos Federais ou Estaduais, Advocacia- Geral da União, Controladoria-Geral da União. A outros órgãos e/ou autoridades podem ser conferidos poderes caso a caso, com a possibilidade de serem utilizados os acordos bilaterais, tratados regionais e multilaterais com base na promessa de reciprocidade (MJ, 2023, p. 2).

2.2 Direito comparado e obtenção de prova digital em nuvem

Os principais *players* do mercado na oferta de nuvem do tipo Platform as a Service (PaaS) ou Plataforma de Serviços em Computação em Nuvem, estão sediados nos Estados Unidos da América (EUA). São eles: Amazon Web Services (AWS), Google Cloud Platform (GCP) e Microsoft Azure (GARTNER, 2023)

Nos EUA, a aplicabilidade legal de pedidos de acesso a evidências digitais de crimes cibernéticos armazenadas em ambiente de nuvem está consolidada atualmente no Electronic Communications Privacy Act (ECPA) – Lei de Privacidade de Comunicações Eletrônicas, de 1986 – e no Cloud Act – Lei de Computação em Nuvem, de 2018 – também conhecida como Lei de Estabelecimento do Uso Legítimo de Dados no Exterior. A primeira atua em nível de agência do governo e pode obrigar provedores de nuvem a divulgarem informações, estabelecer o tipo de processo legal necessário, conforme o tipo de informação pleiteada, além de dispor sobre os limites de privacidade e de proteção aos direitos fundamentais dos cidadãos. A segunda, também de 1986, atualiza o Stored Communications Act (SCA), estatuto federal que concede aos investigadores autoridade para exigir informações mantidas pelos provedores de serviços em nuvem, sujeitos à jurisdição dos EUA.

Porém, a UE, em termos regulatórios, tem papel de destaque, por estar avançando no processo de adoção de iniciativas uniformes entre os Estados-membrosEstados-membros, em pleno atendimento à Convenção de Budapeste. Desde 2016, vêm sendo feitas tratativas para melhoria da justiça penal no ciberespaço, entre as quais, citam-se: propositura de legislação uniforme para os Estados-membros países- membros, por meio de regulamento de acesso transfronteiriço de entrega ou de conservação de provas eletrônicas em matéria penal – proposta n. 2018/0108 (EUR-LEX, 2022) recentemente aprovada sob a designação Regulation (EU) 2023/1543; negociação do Conselho Europeu para adoção do *Cloud Act* dos EUA (WAHL, 2018); e, em 2022, autorização para os Estados-Membros assinarem o segundo protocolo adicional à Convenção de Budapeste, melhorando o acesso transfronteiras a provas eletrônicas e o acesso a evidências digitais fora de sua jurisdição, por intermédio do projeto E-evidence (EUROPEAN CONSILIUM, 2022, p. 2).

Para o escopo deste trabalho, será priorizada a aplicabilidade do SCA dos EUA, que objetivou agilizar o acesso a informações eletrônicas mantidas no país para prestadores globais que investigam crimes graves, como o terrorismo, crimes violentos, cibercrimes e, até mesmo, exploração sexual. Trata-se do marco legal para a atuação investigativa no meio digital, o qual uniformiza o acesso a investigações e as ações penais, com reflexos na validade da prova, complementando a exigência da Convenção de Budapeste (ou do cibercrime).

Essa priorização deve-se ao fato de as principais empresas de tecnologia (*Big Techs*) que também prestam serviços na esfera brasileira – como Microsoft, Google, Facebook, Amazon, Oracle – terem suas sedes principais em território norte-americano, vinculando seus regramentos e programas de conformidade norteadores aos EUA.

Na norma referida, merece destaque a exigência de as companhias sediadas no território americano divulgarem dados que estejam sob seu controle, independentemente de armazenarem os dados em outros países, criando barreiras legais para o pleno cumprimento de requisições oficiais.

Cumpre relatar que, com o advento do Marco Civil da Internet e mais recentemente da Lei Geral de Proteção de Dados Pessoais, o Brasil passou a cobrar de forma mais enérgica que tais empresas, ao comercializarem seus serviços em território brasileiro, cumpram a legislação pátria.

Ocorre que, a despeito de questões técnicas relativas ao formato geograficamente distribuído dos serviços inerentes à computação em nuvem, somadas às lacunas legais na legislação brasileira quanto à temática, mencionadas em capítulos anteriores, essas situações são analisadas individualmente, deixando as autoridades brasileiras em desiquilíbrio quanto à soberania nacional.

A título exemplificativo, cita-se a decisão proferida pelo Ministro Alexandre de Moraes, do Supremo Tribunal Federal, em 17 de março de 2022, na petição n. 9.935/DF, que culminou no bloqueio do aplicativo Telegram, da qual se extrai o seguinte trecho:

> O desrespeito à legislação brasileira e o reiterado descumprimento de inúmeras decisões judiciais pelo Telegram – empresa que opera no território brasileiro, sem indicar seu representante – inclusive emanadas do Supremo Tribunal Federal – é circunstância completamente incompatível com a ordem constitucional vigente, além de contrariar expressamente dispositivo legal.

Dificuldades de se obter a cooperação internacional diante da necessidade de se obterem evidências e provas eletrônicas, na maioria dos casos em prazo exíguo, demandaram a criação do citado Cloud Act, o qual prevê, por meio de acordos/parcerias entre os países, a busca de eficiência frente à grave criminalidade. Esse ato constitui um marco na regulação, uma vez que, simultaneamente, assegura a privacidade e determina critérios de acesso aos dados de empresas de tecnologia globais (ROSA; VIEIRA, 2019, p. 3).

Entre as inovações albergadas pelo Cloud Act, destaca-se a preferência do contato direto com o provedor de serviço de nuvens pelas autoridades brasileiras, em relação ao uso do sistema Mutual Legal Assistance Treaty (MLAT), regulado nos EUA pelo Decreto n. 3.810/2001. Até então, necessitava-se de acordo prévio com o país requisitante. O MLAT fornece assistência jurídica em matéria penal nas relações entre o governo norte-americano e o Brasil; auxilia autoridades brasileiras a obterem acesso a dados pertinentes à investigação em outras jurisdições. Porém, o fluxo dos processos a esses dados, por depender de carta rogatória (via canais diplomáticos), tornava moroso o acesso à evidência e muitas vezes não eficiente. A obscuridade legal possibilitava inúmeras formas de as empresas norte-americanas não atenderem o pedido pelo elevado número de requisições negadas, pela não correspondência à forma ou por algum problema de interpretação da letra da lei.

Ademais, o Cloud Act reforçou a explicabilidade quanto ao escopo geográfico das solicitações de autoridades policiais dos EUA, bem como proporcionou novos meios para os provedores de serviços contestarem solicitações que conflitam com as leis ou os interesses nacionais de outros países, sempre que identificarem que o dado e/ou informação solicitados afetam legislação local ou conflitam com direito fundamental de cidadão americano. Um exemplo disso é a redução da prática de *fishing expedition* ou “procura especulativa, no ambiente físico ou digital, sem ‘causa provável’, alvo definido, finalidade tangível ou para além dos limites autorizados (desvio de finalidade), de elementos capazes de atribuir responsabilidade penal a

alguém” (ROSA, 2021, p. 1). A medida protege a privacidade dos clientes das *Big Techs, Tech Giants, Big Four ou Big Five* norte-americanas (nomes pelos quais são conhecidas as quatro ou cinco das indústrias de Tecnologia da Informação: Facebook, Apple, Microsoft, Amazon e Google (LAVAREDA, 2022, p. 2).

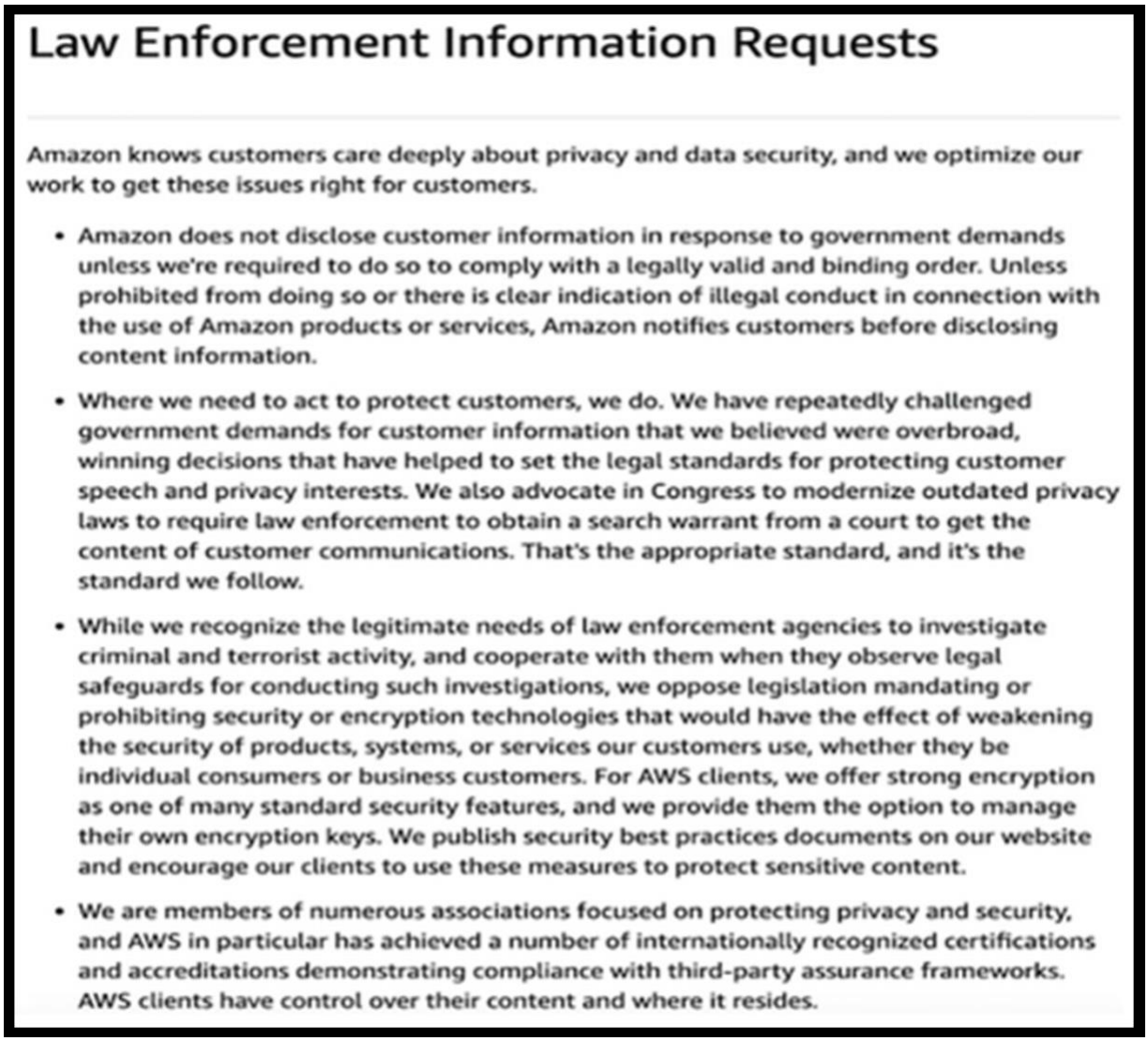
Nesse contexto, as autoridades policiais somente podem solicitar conteúdo de provedores de serviços com o consentimento do cliente ou com um mandado emitido por tribunal, de acordo com os procedimentos criminais dos EUA. Para que o mandado seja emitido, o tribunal deve estar convencido de que há causa provável para acreditar na ocorrência de um crime e que as evidências obtidas nos termos do mandado são diretamente relacionadas a esse crime.

Importa observar que a promulgação do Cloud Act não inviabilizou o uso do sistema MLAT, sendo somente mais um canal de tentativa de obtenção de dados cruciais para solucionar crimes cibernéticos de forma mais ágil e menos burocrática. Inclusive, mesmo com a vigência do Cloud Act, caso o cliente-alvo seja um cidadão ou um residente permanente legal dos EUA e o pedido seja originado de outro país, há necessidade de se utilizar o sistema MLAT para cooperação interna, a fim de garantir as prerrogativas constitucionais do Direito norte-americano e demandando a análise da justiça quanto ao pleito. Segundo Peter Swire e Jeniffer Daskal (2019, p. 5), “O mesmo ocorre com o princípio da reciprocidade em relação a cidadão brasileiro”.

Veja-se que, mesmo com a evolução da legislação local e a criação de tratados de combate ao cibercrime, a prioridade das empresas *Big Techs,* como qualquer negócio, é proteger seus clientes, afinal é deles que extraem a sua fonte de receita.

Nesse sentido, observa-se resistência das *Big Techs* ao pleno cumprimento das leis e tratados vigentes, inclusive com oferta de meios para dificultar ações investigativas, havendo, também, sugestões de o próprio cliente fazer uso da criptografia forte a fim de que a empresa, sendo solicitada a cumprir eventual mandado judicial, forneça dados criptografados às autoridades. Isso dificulta a análise investigativa, como disposto nos Quadros 1 e 2 a seguir, com exemplos de instruções da empresa Amazon Inc., mantenedora do serviço da plataforma em computação em nuvem AWS.

Quadro 1 - Posicionamento da AWS sobre quebra de acesso a conteúdo em nuvem



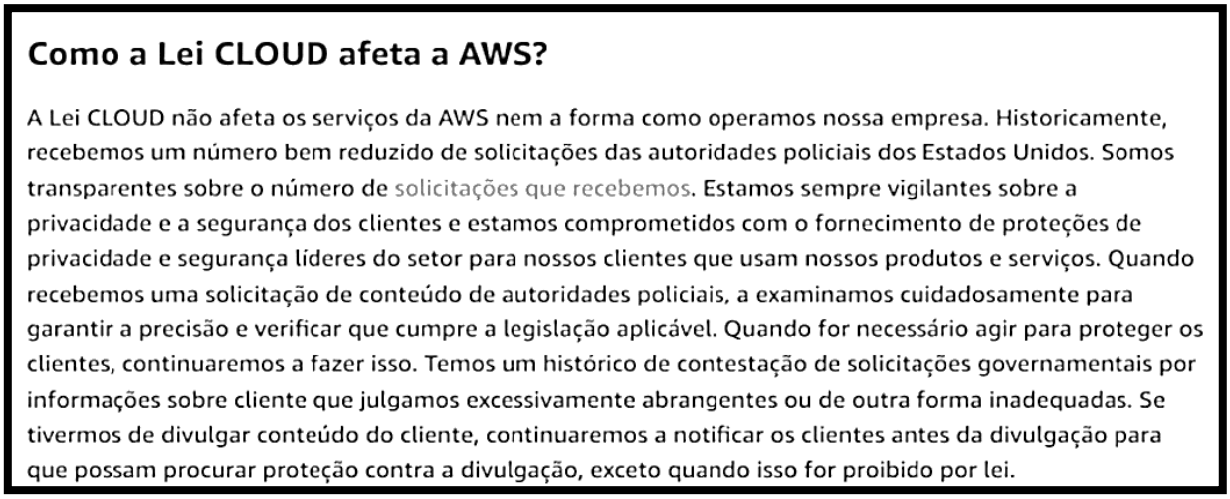
Law Enforcement Information Requests

Amazon knows customers care deeply about privacy and data security, and we optimize our work to get these issues right for customers.

- Amazon does not disclose customer information in response to government demands unless we're required to do so to comply with a legally valid and binding order. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing content information.
- Where we need to act to protect customers, we do. We have repeatedly challenged government demands for customer information that we believed were overbroad, winning decisions that have helped to set the legal standards for protecting customer speech and privacy interests. We also advocate in Congress to modernize outdated privacy laws to require law enforcement to obtain a search warrant from a court to get the content of customer communications. That's the appropriate standard, and it's the standard we follow.
- While we recognize the legitimate needs of law enforcement agencies to investigate criminal and terrorist activity, and cooperate with them when they observe legal safeguards for conducting such investigations, we oppose legislation mandating or prohibiting security or encryption technologies that would have the effect of weakening the security of products, systems, or services our customers use, whether they be individual consumers or business customers. For AWS clients, we offer strong encryption as one of many standard security features, and we provide them the option to manage their own encryption keys. We publish security best practices documents on our website and encourage our clients to use these measures to protect sensitive content.
- We are members of numerous associations focused on protecting privacy and security, and AWS in particular has achieved a number of internationally recognized certifications and accreditations demonstrating compliance with third-party assurance frameworks. AWS clients have control over their content and where it resides.

Fonte: Amazon, 2023.

Quadro 2 - Posicionamento da AWS ao cliente em relação ao cumprimento do Cloud Act



Como a Lei CLOUD afeta a AWS?

A Lei CLOUD não afeta os serviços da AWS nem a forma como operamos nossa empresa. Historicamente, recebemos um número bem reduzido de solicitações das autoridades policiais dos Estados Unidos. Somos transparentes sobre o número de solicitações que recebemos. Estamos sempre vigilantes sobre a privacidade e a segurança dos clientes e estamos comprometidos com o fornecimento de proteções de privacidade e segurança líderes do setor para nossos clientes que usam nossos produtos e serviços. Quando recebemos uma solicitação de conteúdo de autoridades policiais, a examinamos cuidadosamente para garantir a precisão e verificar que cumpre a legislação aplicável. Quando for necessário agir para proteger os clientes, continuaremos a fazer isso. Temos um histórico de contestação de solicitações governamentais por informações sobre cliente que julgamos excessivamente abrangentes ou de outra forma inadequadas. Se tivermos de divulgar conteúdo do cliente, continuaremos a notificar os clientes antes da divulgação para que possam procurar proteção contra a divulgação, exceto quando isso for proibido por lei.

Fonte: AWS, Amazon, 2018

Tais posicionamentos não são exclusivos dessa *Big Tech,* e sim constituem um padrão utilizado pelas principais e maiores plataformas de serviços de computação em nuvem nos EUA. Isso significa que há um entendimento consolidado de que ainda há muito a ser trabalhado para identificação de um formato adequado de atuação investigativa. Essa identificação é que vai possibilitar averiguar e punir os criminosos digitais sem que se ultrapasse a linha tênue dos direitos à privacidade e à liberdade de expressão e dos direitos humanos. Esse é o requisito norteador de todo tratado internacional com Estados Democráticos de Direito.

2.3 Convergência entre o Direito Internacional público e o Direito Internacional privado nos crimes cibernéticos

No decurso das seções anteriores, buscou-se apresentar os desafios e as oportunidades atinentes à admissibilidade de evidências digitais no contexto brasileiro. Para tanto, foram utilizadas como fonte de pesquisa legislações e padrões internacionais adotados por países com maior grau de maturidade na persecução penal de crimes perpetrados em ambientes de computação em nuvem. Tal contexto, de cunho comparativo e orientador, fez-se necessário em razão da natureza transnacional da Internet, dos serviços possibilitados por ela e das resultantes formas de interação sem barreiras geográficas e temporais. Serviços como redes sociais, comunicação eletrônica, aplicativos de comércio eletrônico e outros podem ter sua

hospedagem, armazenamento e processamento prestados em qualquer parte do mundo, não exigindo necessariamente infraestrutura física, presença empresarial ou alocação geográfica em uma única cidade.

Em termos de Direito, no que foi visto até aqui, verifica-se que a abordagem não se encontra limitada a um único viés; aplica-se de forma transversal tanto ao Direito Internacional Privado (DIPr) quanto ao Direito Internacional Público (DIP), justificando a convergência da tratativa entre essas duas vertentes do Direito Internacional.

Na medida em que se utiliza a computação ubíqua como cerne da aplicação do Direito, pode-se segmentar a tratativa e a análise em vários prismas, nos quais as figuras (ou sujeitos de Direito) do Estado, do mercado e do cidadão se entrelaçam e têm suas atribuições e relações jurídicas modificadas.

Assim, no Brasil, por exemplo, se se tem a análise de um contrato de adesão de serviço de computação em nuvem provido por uma das *Big Techs* norte-americanas, busca-se analisar esse contrato na esfera do MCI e do Código de Defesa do Consumidor. Como essa relação jurídica foi estabelecida na perspectiva dos tratados e de acordos internacionais, atinentes e aplicados ao particular (cidadão), passa-se a fazer uso do Direito Internacional Privado.

De outro lado, de forma ampla, ao se analisar a aplicabilidade de um tratado em relação a como o cidadão brasileiro terá seus direitos garantidos, em casos de crimes cibernéticos ocorridos fora do território brasileiro em que esse cidadão é afetado, vem-se utilizar o papel do Direito Internacional Público.

Essa convergência aqui exposta é essencial para o operador do Direito, haja vista que, a depender da percepção escolhida, vários caminhos podem ser trilhados para a concepção de uma estratégia de enfretamento do caso.

No que tange ao Direito Digital, de natureza e abrangência internacionais, os estudos dos internacionalistas devem rumar para uma análise dos instrumentos legais passíveis de serem aplicados ao caso concreto e da possibilidade de adoção de princípios básicos de democracia, soberania, leis e tratados internacionais (VASCONCELOS, 2003, p. 52).

Dan Svantesson (2021), numa análise voltada aos Estados-membros da União Europeia, aponta as questões inerentes ao acesso transfronteiriço de evidências digitais e as minutas de propostas até então em análise pelas comissões e grupos de trabalho voltados a regulamentar a temática.

Ocorre que mesmo num bloco econômico bem estruturado como a UE, ainda há inúmeras divergências legais e culturais quanto ao nível de aplicação de direitos fundamentais, tais como a preservação de direitos humanos e a proteção ao sigilo e à privacidade de seus cidadãos, garantidos pela soberania dos Estados-membros (SVANTESSON, 2021).

Da mesma forma, os EUA também passaram a dispor de legislação específica para regular o acesso a dados armazenados em provedores de nuvem computacional mantidos em território americano, por meio do Cloud Act, mapeando os fluxos e procedimentos que as autoridades policiais e judiciárias deverão seguir para obter o acesso às provas digitais de que necessitam nas investigações para capturar e julgar os cibercriminosos.

Nesse diapasão, importante destacar o significativo avanço recém-conquistado pela União Europeia com a aprovação do Regulamento 2023/1543 do Parlamento Europeu e do Conselho em 12 de julho de 2023.

O novo regulamento aprovado pela UE teve os seguintes regramentos de *vacatio legis*: as novas regras entrarão em vigor em 17 de agosto de 2023 e serão aplicáveis a partir de 17 de fevereiro de 2026 para a Diretiva e de 17 de agosto de 2029 para o Regulamento (UE/CONSELHO, 2023), tempo necessário para que todos os Estados-membros consigam se adequar à uniformização mínima sancionada.

Nessa perspectiva, a existência de uma metodologia previamente normatizada para coleta e guarda de provas digitais (voláteis e intangíveis) constitui uma importante ferramenta para a eficácia da persecução penal. Ante a ausência de previsão legal, a prova digital pode ser vista como uma prova atípica, ou seja, basta “identificar se existem mesmo mecanismos que não se enquadrem no modelo legal, mas que sejam admissíveis no processo como método para se acessar uma fonte de prova e elucidar uma questão fática controvertida” (AMARAL, 2017, apud LEMOS, 2021, p. 18). Desde que sejam obedecidas a legalidade e a licitude, “a prova digital pode integrar o processo e servir como instrumento para aplicação do princípio do livre convencimento

motivado pelo magistrado no momento de valoração das provas. Assim, é nítida a importância da prova digital face o avanço tecnológico” (LEMOS, 2021, p. 29).

No Brasil, com a adesão à Convenção de Budapeste, deve-se iniciar uma fase de evolução do Direito interno, a fim de suprir as lacunas legislativas anteriormente verificadas e de promover uma harmonização normativa relativa a essa Convenção. Visa-se, também e sobretudo, à “potencialização dos instrumentos de cooperação que permitam, de fato, a plena colocação do Brasil em um cenário de integração no cenário internacional de combate aos cibercrimes.” Com isso, também se tornam pauta outros problemas advindos dessa potencialização, a exemplo da proteção aos dados pessoais em investigações criminais, “matéria ainda tortuosa no Direito brasileiro” e, em vários aspectos, dependente de ações legiferantes (PUGLIESE; LUIZ, 2022, p. 4).

Legisladores e a sociedade civil organizada podem discutir questões afetas aos cibercrimes do ponto de vista da legislação penal e processual penal, guiando-se pelo texto da referida Convenção. Inclusive, nesse sentido, por exemplo, grande parte das condutas relativas aos crimes cibernéticos, nela referenciadas, encontra-se tipificada também como crimes na legislação brasileira. Porém, o tratamento penal estabelecido para eles não reflete “o potencial danoso e a complexidade do mundo digital” em que se vive (PUGLIESE; LUIZ, 2022, p. 4).

A esse respeitam, comentam Pugliese e Luiz:

> O delito de invasão de dispositivo informático (art. 154-A do Código Penal) [...] foi introduzido no Direito brasileiro em 2012, mas deixou de ser enquadrado como infração penal de menor potencial ofensivo e teve a sua pena aumentada apenas no ano passado, com o advento da Lei n. 14.155/2021. Isso denota que a harmonização do Direito Penal brasileiro com a realidade dos cibercrimes ainda caminha devagar e exige um esforço mais amplo (PUGLIESE; LUIZ, 2022, p. 4).

A mencionada revisão no Direito interno deve percorrer os tipos penais vigentes e as formas da respectiva responsabilização. Nesse sentido, a Convenção de Budapeste dispõe sobre a necessidade de se disciplinar adequadamente crimes que atentem contra a confidencialidade, a integridade e a disponibilidade de dados em geral e de sistemas de computador. Crimes propriamente informáticos, associados ao conteúdo da informação e à “violação de direitos autorais e de direitos correlatos”. Incluem-se, nesse bojo, meios de responsabilização de pessoas jurídicas (PUGLIESE; LUIZ, 2022, p. 5).

Ressalta-se que os efeitos da mera promulgação legislativa no cenário pátrio não suprem as necessidades atuais, ou seja, não acompanham a evolução digital e, obviamente, a evolução dos crimes cibernéticos. A propósito, lembre-se de que o próprio Direito demora a atualizar-se em relação aos movimentos da sociedade, mormente quanto aos rápidos avanços tecnológicos que se impõem na realidade social de modo irreversível e a seus efeitos nocivos, como o tema discutido neste estudo.

Além disso, no Brasil, especificamente, o excesso de burocracia permeia todos os processos legislativos, a exemplo do Projeto de Lei n. 8045/ 2010, de 22.12.2010, para um novo Código de Processo Penal, de autoria do então senador federal José Sarney (PMDB/AP), que até o presente se encontra em tramitação na Casa de leis, por determinação da Mesa Diretora da Câmara dos Deputados em 20 de abril de 2021: “Prorrogo, de ofício e *ad referendum* do Plenário, por doze sessões a partir de 20 de abril de 2021, o prazo para a Comissão Especial discutir e votar o projeto e as emendas com os pareceres” (CD, 2023, p. 4).

Com base nisso, acredita-se que o uso do desenho regulatório pode vir a ser uma alternativa interessante para suprir as lacunas legais observadas no processo de persecução penal pátrio. A finalidade é garantir minimamente metodologias e mecanismos utilizados pelos órgãos de aplicação de leis, como o Ministério Público e as Polícias Federal e Civil, na obtenção de provas digitais. O respaldo técnico e legal de canais e meios nesse sentido é uma forma de esse tipo de prova ser admitida no processo judicial brasileiro, sem que haja prejuízo no processo persecutório.

É inequívoco que, em não se dispondo no Brasil de mecanismos eficazes de obtenção de provas digitais – como ocorreu em países com democracia consolidada e com respeito aos direitos humanos e à privacidade de dados pessoais –, há de se estabelecer meios complementares para fortalecer a cadeia de custódia de provas digitais e, assim, mitigar os riscos jurídicos de sua inadmissibilidade por ausência de previsão legal. O Direito Internacional e o Direito Regulatório são essenciais à solução do problema.

3 ACREDITAÇÃO E ADMISSIBILIDADE E DE PROVAS DIGITAIS

A valoração da prova passa necessariamente pela observância de quatro fatores principais – autenticidade, integridade, preservação de cadeia de custódia e utilidade –, definidos anteriormente. Este último se refere à qualidade da atividade probatória digital, ou seja, se a prova, por si só, constitui elemento minimamente válido, a fim de não possibilitar sua fácil desconstrução (THAMAY; TAMER, 2020, p. 40).

Para Schauer (2022, apud MALTA *et al*., 2023, p. 189-190), a valoração e a admissão de provas suscitam questões anteriores à atividade probatória, como “a confiança na ciência e [...] a confiança nos peritos forenses”. E inquire diretamente: Como os não especialistas podem saber quem são os especialistas e quem não é? “Como as pessoas que não são treinadas em análise científica forense podem determinar em quais especialistas devem acreditar e em quais não?”. Esses autores trazem para o plano prático os questionamentos de Schauer em outras palavras: “como prevenir a Justiça de deixar-se contaminar pela ciência produzida sem critérios confiáveis, também conhecida como *junk science*? Como saber quando a ciência é confiável ou não?”

Nesse sentido, a valoração da prova digital, além de todas as implicações mencionadas, também demanda atendimento a particularidades técnicas, como volatilidade e fragilidade. Isso porque ela pode ser alterada, editada, manipulada ou até mesmo destruída de modo doloso ou culposo, tanto pelos agentes processuais como pelos peritos.

Também demanda, da parte incumbida de apresentação da prova, o uso de uma linguagem clara e objetiva no laudo pericial e/ou petição, com o fito de se fazer compreender.

Nessa perspectiva, Schauer (2022, apud MALTA *et al*., 2023, p. 191) reflete sobre a necessidade de a perícia atender a critérios objetivos que alcancem a compreensão não só de cientistas e de especialistas, mas também das partes do processo e, principalmente, dos magistrados, aos quais cabe decidir exatamente com base na valoração da prova e na respectiva admissão como tal (MALTA *et al*., 2033, p.191).

Em termos práticos, o perito, as partes e, em especial, o magistrado, a quem cabe a análise da prova, precisam compartilhar uma linguagem comum, pela qual se *façam compreender*. E quando nos referimos a *compreender*, não estamos a sugerir que o magistrado tenha o dever de se aprofundar no conhecimento científico do qual dispõem os peritos – não é essa a ideia. O que se sugere é a importância de que o perito transmita as informações das quais o magistrado precisar dispor para formar sua convicção, inclusive sobre a própria validade e o valor daquela prova pericial para o processo (MALTA *et al*., 2023, p. 190).

A admissão da produção de prova pericial, incumbência atribuída ao juiz, envolve aspectos tênues por si sós, o que é agravado pela ausência de parâmetros objetivos que o auxiliem ou o amparem. A união das tenuidades com a ausência de parâmetros cria um espaço de risco à não admissão da prova pericial em casos em que ela seja essencial à solução do conflito, ainda ofende o direito das partes à prova e prejudica a prestação jurisdicional (MALTA *et al*., 2023, p. 194).

3.1 Valoração e admissibilidade de provas no Judiciário brasileiro

A valoração de uma prova é um ato de difícil controle judicial, haja vista o juiz se pautar por seu convencimento livre e racional, o que implica a apreciação livre das provas como fator de motivação da decisão final acerca de sua admissão ou não. Na maioria das vezes, a interpretação de evidências digitais exige conhecer aspectos que estão além daqueles com os quais o operador do Direito trabalha rotineiramente, abrangendo, inclusive, outras áreas. Como esse é um conhecimento que não se tem, para se evitar arbitrariedades na hora de decidir, é necessário que se estabeleçam critérios que tornem racional a valoração da prova, pautando-se no livre convencimento do juiz. O objetivo é auxiliar sua motivação (MARTINI, 2015, p. 9).

O art. 436 do CPC de 1973, inclusive, determinava: “O juiz não está adstrito ao laudo pericial, podendo formar a sua convicção com outros elementos ou fatos provados nos autos” (MARTINI, 2015, p. 9). Comparativamente, o CPC 2015, no art. 479, estabelece: “O juiz apreciará a prova pericial [...] indicando na sentença os motivos que o levaram a considerar ou a deixar de considerar as conclusões do laudo, levando em conta o método utilizado pelo perito”.

Do exposto, infere-se que o artigo do novo CPC apenas dispõe de forma ampla o que o artigo do CPC 1973 define de modo mais claro, uma vez que, para indicar as razões de seu convencimento (CPC 2015), o juiz precisa se valer de conhecimentos e de outros elementos (CPC 1973).

A produção e a interpretação de evidências digitais podem levar o magistrado à necessidade de designar um profissional especialista na temática específica, o perito. Esse profissional tem, entre suas atribuições, as de identificação, coleta, análise técnica das provas digitais no ambiente do caso concreto e de interpretação analítica dos resultados. Sobretudo, a comunicação desse processo deve ser feita de forma inteligível (COSTA-NETO; TRINDADE, 2023, p. 214).

No contexto criminal, o papel do perito é analisar quanto a evidência científica oferece de suporte às hipóteses da acusação e da defesa, enquanto o julgador avalia se esse suporte provê sua incerteza no que tange a essas hipóteses. Ao perito não cabe falar sobre as hipóteses, cuja avaliação vai depender “da interpretação de todo o conjunto probatório (que inclui provas não científicas)”. Isso já está além da atuação do perito. “O perito se baseia na evidência, mas a evidência (dos leigos) consiste no que o perito disse”, é o que defende Schauer (2022, apud COSTA-NETO; TRINDADE, 2023, p. 215).

Conforme aduzem o art. 181 – “No caso de inobservância de formalidades, ou no caso de omissões, obscuridades ou contradições, a autoridade judiciária mandará suprir a formalidade, complementar ou esclarecer o laudo” – e o art. 182 – “O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte” – do CPP, caberá ao juiz analisar o laudo entregue pelo perito e decidir quanto à sua aceitação ou rejeição no todo ou em parte, bem como sobre a necessidade de complementação e/ou contratação de novo perito. De outra parte, conforme Costa-Neto e Trindade (2023, p. 220), para deliberar quanto ao laudo entregue pelo perito, o magistrado deve ter critérios mínimos “para adotar uma postura cética diante de exames e laudos” de qualquer natureza.

Nesse sentido, João Costa-Neto e Trindade (2023, p. 220) destacam o importante debate sobre a formação do operador do Direito e à respectiva necessidade de se desenvolverem conteúdos em uma visão interdisciplinar. A finalidade é possibilitar conhecimentos essenciais não somente na área de humanas, mas também na área biológica e de exatas. Esses pressupostos encontram-se

expressos na Resolução n. 5, de 17 de dezembro de 2018, da Câmara de Educação Superior do Conselho Nacional de Educação, e foram adotados na Faculdade de Direito da Universidade de Brasília (UnB), em uma disciplina sobre perícia criminal e sobre o sistema de justiça, denominada “Perícia: Justiça pela Ciência”. O objetivo é formar operadores de Direito com uma visão mais completa, preparando-os para decisões seguras à prática do Direito.

Amparado pelo conhecimento técnico, o juiz poderá adotar uma postura cética que não será fruto de meras intuições. É preciso que o juiz entenda, em linhas gerais, como se faz cada exame pericial, suas vantagens e desvantagens, seus pontos fortes e seus pontos fracos. Poderia contribuir para o atingimento de tal desiderato o estudo, desde a graduação em Direito, das Ciências Forenses (COSTA-NETO; TRINDADE, 2023, p.221).

O novo CPC (2015), em seu art. 473, III, permite ao juiz compreender o conteúdo do laudo pericial, uma vez que se exige do perito a exposição do objeto da perícia, a respectiva análise técnica ou científica, o método utilizado devidamente esclarecido, inclusive “demonstrando ser (esse método) predominantemente aceito pelos especialistas da área do conhecimento da qual se originou” (MALTA *et al*., 2023, p. 201). Acrescente-se às informações do perito resposta conclusiva a todos os quesitos, bem como fundamentação em linguagem simples e coerente, sendo-lhe vedado ultrapassar os limites de sua designação, cabendo ao magistrado avaliar o documento gerado e fundamentar seu posicionamento sobre os fatos ali explorados.

Contudo, no Brasil, a ausência de padrões nesse sentido amplia o poder do magistrado na tomada de decisão. Por um lado, permite maior subjetividade na tratativa e no enfrentamento de novas temáticas relativas à evolução e à disrupção tecnológica vivenciadas na sociedade atual, sem que se demandem proposituras de enxertos na legislação pátria, haja vista a complexidade e a demora de aprovação de nova legislação no país. Por outro lado, “dificilmente um juiz enfrenta uma opinião técnica. Contrariar um laudo ainda é polêmico” (COSTA-NETO; TRINDADE, 2023, p. 219), podendo até acarretar prejuízo ao desenvolvimento da carreira. Vê-se, aí, que a subjetividade se encontra nas duas hipóteses: na primeira, em uma decisão que pode ser equivocada e, na segunda, na avaliação pessoal da carreira.

3.2 A confiabilidade dos dados probatórios no ambiente de nuvem computacional

Da referida lição de Thamay e Tamer (2020) sobre a valoração das provas digitais, extrai-se que, para a admissibilidade da prova digital em um processo judicial, é necessária a observância dos três fatores amplamente citados (autenticidade, integridade e confiabilidade), a fim de que a utilização da prova seja considerada válida. Caso não ocorra o preenchimento de algum desses requisitos, a prova se tornará frágil e imprestável para cumprimento de seu objetivo.

A já citada cadeia de custódia visa manter traços, coisas ou vestígios que possam interessar à reconstrução cronológica e comprobatória dos fatos, “com a finalidade de garantir sua identidade, integridade e autenticidade” (BADARÓ, 2018, apud SOUZA, 2021, p.45).

Para Geraldo Prado (2014, p. 86), cadeia de custódia é um “dispositivo dirigido a assegurar a fiabilidade do elemento probatório, ao colocá-lo sob proteção de interferências capazes de falsificar o resultado da atividade probatória”. Duas outras acepções podem ser citadas: a da Portaria n. 82 de 2014, do Ministério da Justiça, e a advinda de sua regulamentação pela Lei 13.964/2019, que inseriu o art. 158-A no CPP.

Aliás, mesmo antes de prevista em lei, “a cadeia de custódia da prova física já se guiava por um conceito e obtinha ainda o seu conteúdo procedimental pelas diretrizes estabelecidas pela Portaria n. 82 de 2014” (SOUZA, 2021, p. 46). Da mesma forma, de modo esparso, havia referências no CPP sobre as respectivas etapas, aspecto que nos leva a refletir sobre a necessidade de um tratamento sistemático do assunto e com detalhes (MAGNO; COMPLOIER, 2021, p. 199). Apenas para ilustrar a afirmativa desses autores, um dos exemplos do CPP:

> Art. 6º - Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
> I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;
> II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;

> [...]
> VII - determinar, se for caso que se proceda a exame de corpo de delito e a quaisquer outras perícias (art. 6º, CPP); art. 11 (acompanhamento dos objetos que interessam à prova aos autos do inquérito), art. 159 e § 1º (realização do exame de corpo de delito), indicação de assistentes técnicos (art. 159, § 3º e § 4º, CPP), art. 159, § 6º, art. 161 (momento de feitura do exame de corpo de delito), art. 162 (autópsia), arts.163 a 166 (procedimento de exumação), art. 168 (complemento do exame pericial), art. 169 (exame de local do crime), art. 170 (guarda de material para eventual nova perícia) [...] (CPP, 2015, p.14).

Devem ser destacadas as dificuldades que a velocidade nos incrementos de dispositivos e de programas de TI trouxeram para a prática forense. Sem tempo de atualização, o que se tem é uma “perícia basicamente reativa”, mas que não invalida, não impede e menos ainda dispensa a aplicação de metodologias consagradas no que se refere à preservação de provas digitais. É justamente por isso que seguir rigorosamente a cadeia de custódia das provas digitais se torna “uma garantia de natureza constitucional e não mera consequência lógica do sistema de preservação do corpo de delito digital” (PRADO, 2021, p.10).

Em relação ao papel da cadeia de custódia em provas ilícitas, Prado (2014, p. 81) se refere à experiência dos EUA, considerando a possibilidade de ela poder contribuir para o debate legislativo brasileiro nesse sentido. É que o sistema americano busca reduzir as complexidades em torno da vedação das ilicitudes, identificando elos entre as atividades diversas, que integram os procedimentos probatórios, visando aferir a valoração da prova. Dessa forma, a interrupção da cadeia de custódia, ainda que por alguma razão admitida, pode resultar na inadmissibilidade da prova. Uma só interrupção pode causar o enfraquecimento da prova ou até destruir sua capacidade nesse sentido. Por isso, a regra é a de envolver o menor número de pessoas no trato das evidências.

Nessa perspectiva, a cadeia de custódia pode ser vista como um dispositivo pronto a instaurar “a fiabilidade do elemento probatório, ao colocá-lo sob a proteção de referências capazes de falsificar o resultado da atividade probatória.” Ela vai funcionar como um remédio contra as crenças de juízes quando da explicitação das respectivas decisões da decisão, não permitindo decisões condenatórias sem a correspondente ocorrência empírica (PRADO, 2014, p. 86).

O perigo de falsificação, erro e de uso indevido ou abuso é especialmente frequente e relevante e, em certa medida, ainda desconhecido. Os vários sistemas jurídicos empenham-se em reagir a essa situação na tentativa de oferecer uma regulação adequada do novo domínio das “provas informáticas” (TARUFFO, 2014, apud PRADO, 2021, p. 18).

Como já destacado, embora sejam muitas e vastas as dificuldades enfrentadas para o estabelecimento de critérios voltados às atividades da prática computacional forense, documentos internacionais de reconhecido valor podem servir de base. Ressalta-se que, em muitos casos, procedimentos vigentes servem de “base concreta para as diligências a serem satisfeitas” (SOUZA, 2021, p. 50).

Mas nesse contexto, vários Projetos de Lei foram apresentados, alguns com propostas mais amplas, outros com propostas mais pontuais. Conhecer seus respectivos conteúdos é importante para se dimensionar, ante as lacunas verificadas, os próximos caminhos da regulação legiferante.

3.3 Projeto de Lei n. 4939/2020

Conforme já mencionado, recentemente o Brasil aderiu à Convenção de Budapeste sobre cibercrimes e, entre os deveres impostos aos Estados-partes, por meio dos termos “Cada Parte adoptará as medidas legislativas e outras [...]” de seus diversos artigos, nos distintos títulos e abrangendo todas as medidas a serem adotadas, requer a harmonização do ordenamento jurídico nacional para atender aos acordos pactuados no tratado.

Nesse passo, destaca-se a recente majoração das penas para crimes digitais, estabelecida pela Lei n. 14.155/2021, e as propostas de atualizações no Código Penal brasileiro, para melhoria da tipificação dos crimes digitais e inovações pleiteadas para o Novo Código de Processo Penal, por meio do PL n. 8045/2010.

A propósito desse PL, alegações dão conta de que há pontos controversos e polêmicos, entre os quais se destacam: o juiz das garantias (art. 14), os novos meios de obtenção de provas e a evolução das tratativas de interceptação telefônica, atualmente albergadas na Lei n. 9.296/1996. Essa lei, ainda vigente, encontra-se desatualizada ante a evolução dos mecanismos de criptografia.

Para o contexto deste trabalho, optou-se por analisar o PL n. 4939/2020, de autoria do deputado Hugo Leal (PSD/RJ), que propõe a atualização do Código Penal, e dispõe sobre “as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências”. A proposta se refere à definição de “princípios e regras para a obtenção e a admissibilidade de provas digitais na investigação e no processo criminais” (CD, 2020, p. 2).

Especificamente em relação a este estudo, pode-se dizer que todos os seus capítulos estão diretamente associados ao objetivo pretendido:

- Capítulo I (Das Disposições Gerais): destacam-se a aplicabilidade da lei e a conceituação de termos técnicos, tais como “metadados”, “prova nato-digital”, “prova digitalizada”, “integridade” e “autenticidade da prova”;
- Capitulo II (Da Prova Digital na Investigação e no Processo Penal): destacam-se as 14 seções para consolidar tratativas quanto a meios de obtenção de provas; interceptação telemática; requisição itinerante; coleta por acesso forçado; decisão judicial e prazo; mandado judicial; termo circunstanciado; cadeia de custódia específica; restituição de dispositivos eletrônicos ou sistemas informáticos; sigilo profissional e religioso; dados íntimos e restrições de acesso à informação; encontro fortuito e serendipidade; infiltração virtual e ação disfarçada;
- Capítulo III (Dos Crimes e das Penas): segmenta-se em 5 seções: falsidade informática; dano informático; sabotagem informática; acesso ilícito; e interceptação ilícita;
- Capítulo III (Disposições Finais): alteram-se os arts. 36, 37 e 38 do Código Penal vigente para nova redação proposta.

Por se tratar de um PL, obviamente o conteúdo ainda será alvo de análises de ajustes na Casa de leis. Contudo, preliminarmente, percebe-se grande inovação na proposição e abertura para a tratativa na persecução penal de crimes cibernéticos, já alinhados às boas práticas publicadas pela International Organization for Standardization (ISO) e pela British Standard Institute (BS). Também há abertura legal para uso de artigos genéricos para adequação em outras tecnologias que porventura também sejam aplicáveis, tal como a redação proposta para a seção de cadeia de

custódia específica, *in verbis*:

> Art. 19 Os meios de obtenção da prova digital serão implementados por perito oficial ou assistente técnico da área de informática, que deverão proceder conforme as boas práticas aplicáveis aos procedimentos a serem desenvolvidos, cuidando para que se preserve a integridade, a completude, a autenticidade, a auditabilidade e a reprodutibilidade dos métodos de análise.
> § 1º A realização da obtenção garantirá, independentemente de norma técnica:
> I - ambiente controlado com redução de contaminação;
> II - espelhamento técnico em duas cópias, com o máximo de metadados e a descrição completa de procedimentos, datas, horários ou outras circunstâncias de contexto aplicáveis;
> III - preservação imediata após o ato de espelhamento com emprego de recurso confiável que garanta a integridade da prova.
> [...]
> Art. 21 Salvo expressa determinação judicial em contrário ou impossibilidade de cumprimento da medida desta forma, a apreensão da prova digital ocorrerá por espelhamento, não se fazendo a apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica (PL n. 4939/2020).

Outro ponto relevante desse PL refere-se à requisição itinerante de que trata o art. 11, possibilitando que um provedor acionado, ao identificar que, para preservação do dado, necessita de outro provedor (terceiro), possa remeter a requisição em caráter itinerante, independentemente de nova ordem, comunicando tal feito, entretanto, à autoridade judicial.

Verifica-se, ainda, que o PL buscou mitigar a pescaria probatória (*fishing expedition*), determinando que os mandados judiciais informem a materialidade, os motivos e as necessidades. É o que dispõe o art. 14, *in verbis*:

> Art. 14 A decisão judicial será instrumentalizada por mandado judicial, dirigido aos seus executores e às pessoas físicas ou jurídicas que irão sofrê-la, suficientemente instruído com informações sobre os fatos sob investigação, a pessoa física ou jurídica alvo da diligência, se possível, os dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, se for o caso, os provedores ou serviços de infraestrutura, de conexão ou de aplicação, potencialmente atingidos, o objeto da medida, os procedimentos autorizados a serem efetuados, os limites da apreensão e o prazo para cumprimento.

> Parágrafo Único Será expedido mandado de intimação aos interessados, nos termos do caput, logo após o fim do cumprimento da medida, desde que não prejudique a operação (PL n. 4939/2020).

É certo que a tecnologia trouxe e continua trazendo preocupações legítimas em relação à tutela da privacidade (art. 5º, X, CF), haja vista a magnitude dos delitos virtuais que necessitam ser combatidos, “sob pena de violação do princípio da vedação da proteção deficiente estatal, como decidiu a Corte Interamericana de Direitos Humanos (CIDH), no caso Ximenes Lopes *vs*. Brasil, em 2006”. Nesse caso, o Estado foi condenado sob o argumento de, apesar de não ter violado diretamente um direito determinado, não adotou as necessárias medidas de prevenção nem efetuou “uma investigação séria, por um órgão independente, autônomo e imparcial” (LAI; MOURÃO, 2021, p. 5).

Contudo, mesmo com os esforços envidados para harmonizar a legislação brasileira ao contexto internacional e com a tramitação de propostas para um novo Código de Processo Penal, infere-se que, ainda assim, será necessário o uso de desenho regulatório específico, com fins de atuação complementar da legislação, de forma análoga ao ocorrido no cenário norte-americano, devido à ubiquidade do mundo digital e à evolução exponencial dos cibercrimes, entre os quais, cita-se o sequestro virtual de dados (*ransonware*), além dos inúmeros outros que surgirão até a promulgação das novas leis. O *ransonware,* apesar da extensa e crescente ocorrência, ainda não foi coberto pelos PLs em tramitação,

3.4 Projeto de Lei n. 4291/2020

O PL n. 4291/2020, proposto pela então deputada federal Margarete Coelho (PP/PI) (CD, 2020a), tem como objeto a alteração do CPP, para dispor: sobre a custódia dos elementos digitais de prova, em complemento a seu Capítulo II - Do Exame de Corpo de Delito, da Cadeia de Custódia e das Perícias em Geral (atualizado pela Lei n. 14.964/2019); novas designações para o art. 158 com 10 insertos (letra G a letra P), detalhando os requisitos para acesso e tratamento de informações digitais apreendidas. Visa possibilitar a certificação de integridade, da origem e da destinação da evidência digital coletada, com o fito de atribuir credibilidade e acreditação ao elemento probatório colhido como evidência digital.

Desse PL, pode-se inferir que a autora, além de conceituar a cadeia de custódia de elementos digitais, adentrou os procedimentos mínimos que devem ser tomados para instrução de mandados de busca e apreensão, bem como os cenários de exceção a serem considerados em casos de urgência que envolvam risco de vida ou privação de liberdade.

No que tange a este estudo, destacam-se as tratativas dispostas nas redações dos arts. 158-G a 158-I, *in verbis*:

> Art.158-G. A cadeia de custódia dos elementos digitais, contidos em sistemas computacionais, deve ser garantida por meios tecnológicos adequados que permitam a produção de cópias dos dados originais preservando sua integridade e garantindo a impossibilidade de sua modificação, viabilizando, sempre que possível, a continuidade do uso dos sistemas e serviços informáticos por seus legítimos proprietários.
> Art. 158-H. **A cadeia de custódia dos elementos digitais deverá ser realizada por meio de protocolos que permitam aferição dos critérios de tratamento, preservando-se a integridade, a completude, a autenticidade, a auditabilidade e a reprodutibilidade dos métodos com que foram obtidos** os dados garantindo a não alteração dos dados custodiados.
> Art.158-I. Quando vestígios digitais forem recolhidos pelo seu potencial interesse para a produção de provas, **deve o agente responsável pela sua custódia realizar todos os protocolos para garantir sua preservação, sua não alteração e seu sigilo, sendo vedado o acesso aos dados contidos no material sem prévia autorização judicial**. (grifos nossos)

Pela leitura dos artigos supracitados, pode-se ratificar a postura do legislador em sugerir adoção de protocolos para garantia da inviolabilidade das provas digitais coletadas. Tais protocolos, segundo entendimento particular, não foram pormenorizados por ser ampla a utilização de artefatos digitais passíveis de coleta. Tal condição possibilita complemento regulatório quanto a quais protocolos e/ou métodos devem ser utilizados pelas autoridades policiais, de forma a garantir os princípios de segurança previstos na legislação (integridade, autenticidade, confidencialidade, auditabilidade, reprodutividade).

Nesse sentido, entende-se que há necessidade de estabelecimento de regulações e/ou metodologias acreditadas a serem realizadas pela força policial no decurso de todo o processo de coleta, armazenamento e acesso às provas digitais apreendidas, pois há risco de serem invalidadas em caso de adoção de métodos/protocolos não documentados e/ou não acreditados tecnicamente.

Todavia, apesar dos esforços para tentar legitimar o referido PL no sentido de alterar o CPP vigente, o projeto se encontra, desde 08/03/2021, pendente de análise na comissão especial responsável pela atualização do CPP, juntamente com outras proposituras de atualizações.

3.5 Projeto de Lei n. 1515/2022

O PL n. 1515/2022, de iniciativa do então deputado Coronel Armando (PL-SC), conforme prevê o disposto no inciso III e no § 1º do art. 4º, tem como finalidade regular o uso de dados pessoais em atividades de investigação e de repressão de infrações penais não cobertas pela Lei n. 13.709/2018 – a Lei Geral de Proteção de Dados Pessoais. O PL teve forte incidência em tratativas inicialmente colacionadas ao anteprojeto dessa lei, desenvolvido por juristas no decurso de 2020.

Esse projeto é estruturado em 9 capítulos com 59 artigos e tem como objetivo primário o atendimento a três pilares citados no art. 1º, quais sejam: I - proteger os direitos fundamentais de segurança, liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural; II - assegurar a eficiência da atuação dos órgãos incumbidos das atividades de defesa nacional, segurança pública e de investigação e repressão de infrações penais; III - possibilitar o intercâmbio de informações de dados pessoais entre autoridades competentes no exercício das atividades de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais.

A esta pesquisa, interessam especialmente os seguintes artigos, *in verbis*:

> Art. 27. O direito à retificação de dados pessoais não alcançará informações baseadas em percepções pessoais colhidas por agentes de autoridades competentes e testemunhas
> [..]
> Art. 30. Os agentes de tratamento devem adotar **medidas de segurança, físicas, técnicas e administrativas,** aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

> § 1º A ANPD poderá dispor sobre **padrões técnicos mínimos** para tornar aplicável o disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do artigo 4º desta Lei.
> [...]
> Art. 31. Os sistemas desenvolvidos, a partir da vigência desta Lei, para o tratamento de dados pessoais devem ser estruturados de forma a **atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares**. (grifos nossos)

Do conteúdo acima depreende-se o risco de impossibilidade de retificação de dados nas condições previstas no art. 27, qual seja, a aceitação de percepções pessoais de terceiros, dando azo a riscos discriminatórios e à impossibilidade do contraditório pelo próprio titular do dado. Noutra esteira, destacam-se os grifos na redação dos arts. 30 e 31 supra, que impõem a necessidade de complementação regulatória proposta para o pleno atendimento à proteção de dados pessoais.

O PL n. 1515/2022 ainda se encontra em fase inicial de tratativas na Câmara dos Deputados, aguardando a criação de comissão especial da mesa diretora para dar início à análise e aos debates internos quanto às mudanças nos artigos inicialmente propostos.

3.6 Análise da legislação internacional

No contexto da legislação internacional, destacam-se a regulação e as diretivas transfronteiriças adotadas pela UE, com o objetivo de unificar e de otimizar procedimentos legais para combate a crimes cibernéticos entre os Estados-membros e a legislação atualmente vigente nos EUA (UE, 2023, como o citado exemplo da adoção do Cloud Act, em discussão desde 2018.

De acordo com as novas regras, as autoridades judiciais poderão solicitar diretamente provas eletrônicas a prestadores de serviços – como empresas de telecomunicações ou de redes sociais sediadas noutro Estado-Membro. Os prestadores de serviços serão obrigados a responder no prazo de 10 dias, ou de 8 horas em casos de emergência. Por meio de uma ordem de preservação europeia, as

autoridades judiciais podem impedir que prestadores de serviços estrangeiros apaguem dados. Isso permitiria às autoridades solicitar essas informações numa fase posterior. Os prestadores de serviço que atuem na UE devem nomear um representante legal ou designar um estabelecimento para o qual as autoridades judiciais possam enviar as suas ordens de obtenção de provas eletrônicas. O seu papel será a recepção, o cumprimento e a execução das ordens europeias de produção e conservação. O representante legal terá de estar fisicamente presente na UE. Tanto o estabelecimento, ou seu representante legal designado, quanto o próprio prestador de serviço poderão ser responsabilizados caso não cumpram as determinações. Os Estados-Membros devem certificar-se de que existem sanções em caso de incumprimento (UE, 2023, p. 2-3).

Em 14 de junho de 2023, o Conselho da União Europeia apresentou a proposta do "Regulamento Relativo às Provas Eletrônicas: Ordens Europeias de Produção e de Conservação para Efeitos de Provas Eletrônicas em Matéria Penal", que versa que ordens europeias de produção e de conservação de provas eletrônicas sejam obrigatórias em todos os Estados-membros e aplicáveis 36 meses após sua entrada em vigor. Embasado em vários documentos anteriores, o Regulamento foi aprovado com breves alterações e passou a constituir a posição do Parlamento sobre o assunto. “A posição do Parlamento reflete o que havia sido previamente acordado entre as instituições” (UE/CONSELHO, 2023, p. 2).

Entre os vários documentos previstos nesse Regulamento, encontra-se a Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho, formalizada em 12 de julho de 2023, “que estabelece regras harmonizadas aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais para efeitos de recolha de prova eletrônica em processos penais” (UE/PARLAMENTO, 2023, p. 1), incluindo a preservação de evidências digitais no decurso de processos investigativos.

Já as diversas tratativas abordadas no Regulamento incluem a análise quanto ao enquadramento legal do documento na legislação vigente nos Estados-membros e o atendimento aos tratados internacionais já pactuados, tal como a Convenção de Budapeste.

A fragmentação do quadro jurídico cria problemas às autoridades responsáveis pela aplicação da lei e às autoridades judiciais, bem como aos prestadores de serviços que procuram satisfazer pedidos lícitos de provas eletrônicas, uma vez que se

deparam cada vez mais com insegurança jurídica e, potencialmente, conflitos de leis:

> [...] o presente regulamento deverá complementar a legislação da União em vigor e clarificar as regras aplicáveis às autoridades responsáveis pela aplicação da lei e às autoridades judiciais, bem como aos prestadores de serviços no domínio das provas eletrônicas, assegurando simultaneamente o pleno respeito dos direitos fundamentais (UE/ PARLAMENTO, 2023, p. 11).

Nas 224 laudas que compõem o Regulamento, pode-se obter desde a conceituação dos princípios balizadores da regulação e de termos técnicos, até o regramento processual para resoluções de conflitos atinentes à privacidade de dados e às garantias de direitos humanos.

Já nos EUA, as questões relativas à temática são fundamentadas no *common law* com sólido uso de The Federal Rules of Evidence ou Regras Federais de Evidência, adotadas em grande parte dos estados norte-americanos. Essencialmente, essas regras estabelecem os seguintes princípios basilares: autenticidade da prova digital e garantia da cadeia de custódia (considerados indissociáveis) e confiabilidade da prova no contexto processual (GOODISON *et al*., 2015, p. 10).

A autenticidade se refere ao processo de confirmar “que a evidência é realmente o que é e o que os proponentes afirmam que sim”. Geralmente, um ponto específico na autenticação de evidências digitais envolve verificar a identidade do autor dos registros eletrônicos. [...] “As Regras Federais de Evidências [...] permitem que a autenticação possa ser estabelecida através do depoimento de uma testemunha experiente”, tal como um agente policial que, tendo apreendido um aparelho celular ou outro equipamento, “é capaz de testemunhar de onde os arquivos foram retirados” (GOODISON *et al*., 2015, p. 11).

Cotejando a visão norte-americana sobre o quesito tratamento das provas/ evidências digitais com a visão da UE, por exemplo, destaca-se a importância dada pelas cortes norte-americanas ao testemunho técnico do perito forense, com fundamento na regra n. 702 da Federal Rules of Evidence, o que não foi observado na UE, pelo menos nos documentos consultados nesta pesquisa. Esse testemunho, em alguma situação ou condição, pode servir de solução, lembrando-se aqui a importância da responsabilidade dos agentes técnicos envolvidos no processo.

A cadeia de custódia garante que as evidências digitais foram preservadas em seu formato original. Implica a capacidade de se documentar quando e onde as provas

foram coletadas (tipo, identidade propriedade e propriedade do dispositivo), quem era o proprietário do dispositivo e quem teve acesso a ele. Também implica como as evidências foram coletadas (ferramentas e procedimentos usados). Finalmente, cadeia de custódia envolve documentar como as evidências foram armazenadas, quem lidou com as evidências e quem teve acesso a elas (GOODISON *et al*., 2015, p. 12).

Na UE, o citado “Regulamento Relativo às Provas Eletrônicas: Ordens Europeias de Produção e de Conservação para Efeitos de Provas Eletrônicas em Matéria Penal” não trata especificamente da cadeia de custódia. Como diz respeito a questões mais gerais na busca de uma possível uniformização de padrões de tratamento da matéria, o documento se refere à Diretiva 2014/41, que estabelece procedimentos e prazos, reconhecendo que esse documento e a Convenção Relativa ao Auxílio Judiciário Mútuo em Matéria Penal “podem não ser adequados para as provas eletrônicas, que são mais voláteis e podem ser mais fácil e rapidamente apagadas”. Com isso, justifica que “a obtenção de provas eletrônicas [...] é muitas vezes morosa, resultando em situações em que indícios posteriores já não estejam disponíveis” (UE/PARLAMENTO, 2023, p. 10).

O Regulamento admite não haver “um regime harmonizado claro para a cooperação com os prestadores de serviços” e que “os Estados-Membros dependem cada vez mais de canais voluntários diretos de cooperação com os prestadores de serviço, quando existam, e aplicam instrumentos, condições e procedimentos nacionais diferentes”. No que se refere a dados de conteúdo, enquanto “alguns Estados-membros adotaram medidas unilaterais, outros continuam recorrendo à cooperação judiciária” (UE/PARLAMENTO, 2023, p. 10).

Sobre a confiabilidade, nos EUA as Regras Federais de Evidência determinam que esse fundamento deve estar presente em depoimentos científicos e periciais, no conjunto dos princípios gerais e métodos utilizados pelo especialista e na aplicação de princípios e métodos aos casos específicos. Inclusive, um dos testes originais já utilizado na admissibilidade de evidências científicas foi o Frye Test*,* que no caso *Frye vs Estados Unidos*, de 1923, permitiu que determinada evidência fosse admitida “se a ciência na qual ela se baseava fosse aceita pela comunidade científica de modo geral” (GOODISON *et al*., 2015, p. 12).

Porém, visando suprir lacunas metodológicas relativas à confiabilidade do método utilizado para todo o processo de coleta e tratamento das evidências coletadas no processo, o *National Institute of Standard and Technology* (NIST) dispõe de conjunto de padrões a serem utilizados para cada tipo de artefato digital e contexto (sanitização de mídias), com o fito de nortear o perito técnico na acreditação dos métodos que melhor se amoldam ao caso concreto trabalhado. Esse guia ajuda organizações e proprietários de sistemas a tornarem práticas decisões de sanitização baseadas na categorização de confidencialidade de suas informações" (NIST, 2014, p. 1).

Na UE, tal como a cadeia de custódia, o referido "Regulamento Relativo às Provas Eletrônicas: Ordens Europeias de Produção e de Conservação para Efeitos de Provas Eletrônicas em Matéria Penal" também não fala especificamente da confiabilidade, uma vez que, como já esclarecido, esse documento aborda tentativas de uniformizar procedimentos de entrega ou de conservação de provas eletrônicas em matéria penal. Também como já dito, é reconhecida a dependência dos Estados-membros em relação a canais voluntários de cooperação e de utilização de procedimentos.

No cenário norte-americano, dada a massiva adoção de plataformas de serviços em nuvem de computadores, para prover a sustentação da infraestrutura computacional de redes sociais, portais e outras aplicações por empresas de Tecnologia da Informação (*Big Techs* e outras), como já referido, a legislação vigente para coleta, extração e acesso a evidências digitais se encontra consolidada no ECPA e no já citado Cloud Act.

4 REGULAÇÃO COMO MEIO DE ACREDITAÇÃO E ADMISSIBILIDADE DE PROVAS DIGITAIS

Ficou claro, no decorrer da abordagem deste estudo, o papel da cadeia de custódia em relação à garantia do contraditório e do direito de defesa, mormente quando se trata de ocorrências no ambiente digital. Porém, a Lei n. 13.964/2019 não dispôs sobre a inclusão de outras provas que não as físicas. E nesse aspecto, é difícil utilizar “alguma espécie de analogia a equiparar essas espécies probatórias, eis que essencialmente distintas, o que traria uma solução quase sempre inadequada” (SOUZA, 2021, p. 50).

Quatro princípios são passíveis de utilização como norteadores da atividade forense de investigações criminosas: o primeiro é endereçado aos agentes estatais, os quais não devem realizar nenhuma alteração no material colhido e que será posteriormente levado ao Tribunal; em segundo lugar, deve-se ter pessoas capacitadas e especializadas para ter acesso aos dados ou ao armazenamento do dispositivo; um terceiro princípio dispõe que, por meio dos dados fornecidos, seja possível um terceiro (perito) reavaliar os dados e chegar a mesma conclusão técnica; por fim, para que esses princípios sejam devidamente seguidos, requer-se que a pessoa responsável pela investigação seja encarregada de fazer valer toda a metodologia pertinente, inclusive dos preceitos em questão (MENDES, 2020, apud SOUZA, 2021, p. 52).

O Estado deve criar regras que orientem os comportamentos humanos nas mais diversificadas situações da vida cotidiana, a fim de permitir a manutenção do convívio social e o desenvolvimento nacional, inclusive e principalmente para identificar crimes e punir os criminosos que abalam a estabilidade social. Essa função se refere à regulação, que, por sua vez, diz respeito a controle e à respectiva abrangência em relação a determinada finalidade, ou seja, regulação/controle, em qualquer caso, implica a observação de limites. Como exemplo nesse sentido, talvez se possa citar, equiparadamente, o “Regulamento Relativo às Provas Eletrônicas: Ordens Europeias de Produção e de Conservação para Efeitos de Provas Eletrônicas em Matéria Penal” (2023) da UE (visto acima). Ele busca uniformizar entendimentos entre os Estados-membros quanto à produção e à preservação de provas eletrônicas, mas reconhece haver dependências por parte de alguns Estados, aplicação de

instrumentos e de procedimentos diferentes por parte de outros e, ainda, medidas unilaterais relativas a outras questões, a exemplo dos conteúdos.

Sobre seu conceito, naturalmente impreciso, a origem da regulação “é de difícil sistematização”, uma vez que sua denominação tem relação com uma “conceituação progressiva”, de conteúdo mais vago e mais impreciso, apesar de bastante utilizado (OLIVEIRA, 2014, p. 1199). Por isso, conhecer teoricamente características da regulação é necessário para delimitar propostas de controle de determinadas ações em relação a alguma matéria.

Notadamente, a regulação lida com duas dificuldades principais: uma é a incerteza e, a outra, a dificuldade em se delimitar os campos de atuação da própria regulação. A primeira refere-se à imprevisibilidade, tanto de comportamento dos componentes reguladores quanto dos resultados da utilização desses mecanismos de ajustamento. A segunda, por sua vez, deve-se à incerteza da definição das fronteiras de atuação dos diferentes componentes reguladores (OLIVEIRA, 2014, p. 1200).

Mas o conceito de regulação também é abrangente. Ela pode ser considerada como um “mecanismo técnico voltado à preservação de uma constante em meio a perturbações exteriores para alcance de estabilidade” (LOPES, 2018, p. 161) ou, ainda, como qualquer ação, técnica ou intervenção em um sistema, seja uma máquina, um organismo, uma associação ou um segmento, para que ele se comporte de uma maneira desejada e de forma perene.

Relativamente à regulação jurídica, o conceito, no Direito, pode ser verificado com base em dois pontos de vista fundamentais: como meio de regulação dos comportamentos e como um sistema. A regulação vai se referir “aos meios de eliminação de contradições e de reforço de coerências”, destacando-se aí uma função dinâmica de equilíbrio que visa sempre à melhoria daquilo a que ela se refere (OLIVEIRA, 2014, p. 1201).

No Direito, busca-se, com a regulação, a edição de normas para possibilitar a vida em sociedade e a resolução dos conflitos. Por isso, o apego à lei, limitadora do poder estatal e expressão de vontade da população, consolidou a ideia de que a legislação poderia normatizar todos os aspectos da vida do homem, sendo ela capaz de trazer a ordem e a paz social (DIAS; SILVA, 2017, p. 39).

Se as normas de uma ordem jurídica regulam a conduta humana (KELSEN, 1998, p. 22), a regulação pode ser entendida como uma ação dinâmica estatal, caracterizada pela limitação do exercício da atividade regulada por meio de políticas que visam ao interesse coletivo e a determinados comportamentos do agente atingido pelo processo (PLACHA, 2007, p. 19).

Por meio da regulação, exterioriza-se o princípio da legalidade. A lei é, simultaneamente, fundamento e limite de atuação do Estado e deve atender aos princípios, aos objetivos e aos fundamentos do texto constitucional (FERREIRA FILHO; FERREIRA, 2016, p. 126). Com a legalidade, o Estado tem legitimidade para regulamentar os comportamentos humanos e intervir nas atividades do mercado e na própria ordem econômica. Em virtude disso, os agentes do Estado encarregados da regulação devem analisar todas as opções e optar pela melhor alternativa para a coletividade.

4.1 Regulação, Estado regulador e função normativa no Judiciário brasileiro

Tradicionalmente, a regulação consiste em assegurar o equilíbrio entre direitos e obrigações, buscado pela lei. Dentro disso, atribui-se ao Estado “o papel de comandar diretamente os atores sociais, estabelecer as *‘règles de jeu’* e garantir que elas sejam respeitadas”. E nesse sentido, a primeira atividade da regulação é eminentemente política, diretamente relacionada ao Executivo e ao Legislativo. A segunda atividade é desenvolvida com base e por meio dos princípios da neutralidade, da equidade e da humanidade – aspectos que, de certo modo, têm relação com as tarefas de um juiz (OLIVEIRA, 2014, p.1202).

Numa perspectiva mais restrita, “regulação é a criação de normas jurídicas que vão disciplinar o exercício de certas atividades, ou seja, é um acesso especial a determinados bens (exercício de algumas atividades comerciais, por exemplo)”. A regulação constitui, desse ponto de vista, a “mão invisível” que impede a autorregulação em vários sentidos – de mercado, de confisco do Estado frente a uma ampla intervenção, entre outros –, abarcando um escopo mais amplo na área jurídica. A regulação não se refere só a corrigir distorções, mas é um instrumento político de caráter social (OLIVEIRA, 2012, p. 1202).

“Ao se observar os diversos sistemas jurídicos no tempo, é possível verificar-se a presença constante do fenômeno regulatório, mesmo considerando-se o risco de se ler o passado com os referenciais do presente” (HESPANA, 2015, apud PEREIRA, 2016, p. 4). Historicamente, como já dito, o Direito tem como principal função regular condutas e solucionar conflitos. Na atualidade, o que distingue a regulação como é vista hoje da regulação tradicional é o reconhecimento cada vez maior da necessidade dessa função, bem como da necessidade da presença de um Estado regulador. Isso porque as circunstâncias do tempo histórico, associadas ao exercício do poder político e ao desenho institucional – esse voltado para a prestação de serviços de utilidade pública –, exigem essa “mão invisível”. Inclusive, essa última característica é que dá mais visibilidade ao papel estatal, imprimindo, ao mesmo tempo, mais importância à sua função regulatória (PEREIRA, 2016, p. 4).

No Brasil, a regulação passou a ter maior visibilidade a partir da criação do Conselho Nacional de Justiça (CNJ) em 8 de dezembro de 2004, por meio da Emenda Constitucional n. 45/2004, que oficializou a Reforma do Judiciário. Esse órgão “é responsável pelo controle administrativo, financeiro e disciplinar do Poder Judiciário brasileiro, exceto do Supremo Tribunal Federal (STF). Suas funções incluem planejar, auxiliar e acompanhar políticas públicas (CNJ, 2023, p. 2).

Discussões sobre as funções e os limites das atividades normativas do CNJ geralmente têm se restringido a seu poder de regular. Nesse sentido, são citados o princípio da legalidade e “a impossibilidade de regulamentos autônomos ou independentes no Direito brasileiro”, à exceção das previsões do art. 84 da Constituição Federal, relativas a assuntos que competem exclusivamente ao presidente da República, ou de decisões do STF na Ação Declaratória de Constitucionalidade n. 12. Essa ADC reconheceu o “poder normativo” primário do Conselho Nacional de Justiça. Há “discricionariedade na edição das resoluções do CNJ, as quais “teriam como limite as matérias reservadas à lei por expressa disposição constitucional” (PEREIRA, 2016, p. 34).

A respeito desse reconhecimento na citada ADC, o respetivo ato normativo – que "disciplina o exercício de cargos, empregos e funções por parentes, cônjuges e companheiros de magistrados e de servidores investidos em cargos de direção e assessoramento, no âmbito dos órgãos do Poder Judiciário e dá outras providências” – foi considerado constitucional pelo STF por maioria dos votos, sob os seguintes

argumentos justificadores:

I - o Conselho Nacional de Justiça (CNJ) tem competência constitucional para zelar pela observância do art. 37 da Constituição e apreciar a validade dos atos administrativos praticados pelos órgãos do Poder Judiciário (inciso II do § 4º do art. 103-B da CF/88);

II - a vedação ao "nepotismo" é regra constitucional que decorre dos princípios da impessoalidade, igualdade, moralidade e eficiência administrativa;

III - além de estar subordinado à legalidade formal, o Poder Público fica adstrito à juridicidade, conceito mais abrangente que inclui os comandos diretamente veiculados pela CF;

IV - a Resolução n. 07/2005, do CNJ, não prejudica o necessário equilíbrio entre os Poderes do Estado – por não subordinar nenhum deles a outro –, nem vulnera o princípio federativo, dado que também não estabelece vínculo de sujeição entre as pessoas estatais de base territorial.

V – [...] no tocante ao mérito, a acionante pugna pelo reconhecimento da constitucionalidade da resolução em causa (STF/ADC n. 12, 2008, p. 5-6).

Inclusive, esse poder normativo primário que confere força de lei às Resoluções do CNJ é comparado ao que ocorre com as resoluções do Tribunal Superior Eleitoral (TSE). Mas os citados debates, embora também busquem fixar “todos os limites ao poder regulamentar” do CNJ, terminam inconclusivos, sem impor coisa alguma. Nega-se o fundamento dos “poderes instrumentais implícitos”, afirmando-se a inconstitucionalidade da “concretização normativa primária de mandamentos constitucionais por Resoluções” (PEREIRA, 2016, p. 34).

É evidente o trabalho do CNJ no desenvolvimento de atividades empíricas verificáveis na administração do sistema judiciário, cujos efeitos têm sido concretos. Quantitativa e qualitativamente falando, seus instrumentos mais presentes são os inúmeros atos normativos, a exemplo das mais de 200 Resoluções de seu órgão plenário, inclusive direcionadas também a outros entes. Com isso, o CNJ erige-se “como órgão regulador do judiciário brasileiro, com claras funções de planejamento e de acompanhamento conjuntural da realidade de atuação do Judiciário” (PEREIRA, 2016, p. 3). Conclui-se então que atividades tidas como tipicamente estatais e

representativas da soberania, como é a atividade jurisdicional, podem e devem ser reguladas. O debate que se põe é como regulá-las em arranjo institucional constitucionalmente válido. Atente-se que, na regulação da atividade exercida pelos entes privados, defende-se e discute-se a autonomia das autoridades encarregadas da regulação (PEREIRA, 2016, p. 6).

Nesse sentido, salienta-se ainda importante lição de Aranha (2023, p. 70) em diferenciar as técnicas de regulação da teoria regulatória.

As técnicas de regulação diferem da teoria regulatória, pois esta implica ordená-las funcionalmente. Coisa inteiramente distinta é a estratégia regulatória, que pode fazer uso de diversos modelos ou teorias. Para fins de maior clareza do discurso, os termos “teoria/modelo regulatório”, “técnica/instrumento regulatório”, “estratégia/modelagem regulatória” e “forma/modo/modalidade/mecanismo regulatório” detêm significados próprios e relevantes para a compreensão do universo regulatório.

Instrumentos ou técnicas regulatórias são meios de que o Estado lança mão com a finalidade de influenciar o comportamento social para alcance dos objetivos inscritos em políticas públicas. Tais meios, sob o enfoque jurídico, configuram-se em instituições de direito público e institutos de direito privado, enquanto cristalizações de cultura jurídica estabilizadas no ordenamento jurídico e na prática institucional de um país. Uma concessão, por exemplo, é uma técnica contratual e estatutária de prestação de serviços públicos.

Estratégias regulatórias dão um passo além, pois gravadas pela característica funcional de integração de instrumentos/técnicas regulatórias à procura de influenciar o comportamento social. Enquanto os instrumentos/técnicas regulatórias podem ser concebidos como despidos de direção sistêmica, as estratégias regulatórias representam um esforço de modelagem, mediante integração de instrumentos e técnicas em uma apresentação inovadora (ARANHA, 2023. p. 70).

Assim, a regulação voluntária, como forma regulatória promovida pelas empresas *Big Techs,* identifica um conjunto de técnicas regulatórias capazes de reforçar os códigos normativos próprios (ARANHA, 2023, p. 72). Contudo, Tendo em vista o mercado voltado a soluções de Internet não ser regulado, por características basilares de descentralização mercadológica, infere-se pela utilização da

autorregulação com constrangimento estatal, também conhecida como autorregulação regulada, como uma alternativa viável à disrupção e ubiquidade tecnológica presentes nesse nicho de atuação.

Do exposto, infere-se que atividades essencialmente privadas também podem – e até devem em certos casos (como o enfocado neste trabalho) – ser alcançadas por uma por regulação geral – em nível de consumidor, em questões ambientais e outras – e por alguma regulação setorial – como especificamente o setor de TI. As necessidades impõem soluções mais gerais ou mais específicas, e as demandas reclamam do Direito.

4.2 Normas internacionais aplicáveis à temática

A rápida evolução tecnológica e as limitações na produção de regulações e de tratados internacionais, capazes de possibilitar o acesso a dados e/ou informações armazenadas fora da jurisdição de determinado país e/ou que englobem múltiplas jurisdições, sem que isso quebre os direitos basilares e fundamentais dos cidadãos, constituem um desafio em razão da natureza global e transfronteiriça das operações atuais (redes sociais, nuvens computacionais e outros).

Nessa perspectiva, como já dito, os países da UE encontram-se na vanguarda com a recente regulação de procedimentos para requisições de evidências digitais em provedores de serviços que compõem os Estados-membros (UE, 2023, p. 4). Essa regulamentação possibilitará unificar processos e fluxos a serem adotados pelas autoridades judiciais na persecução penal de crimes e ilícitos ocorridos fora de sua jurisdição.

De outra banda, com o crescimento do uso de plataformas de serviços de nuvens computacionais, a referida ISO publicou um modelo de confiabilidade para garantia de processamento de dados oriundos de múltiplas fontes, recurso comumente utilizado em plataformas como AWS, Google Cloud, Microsoft Azure. Para ampliar a disponibilidade de seus serviços, essas plataformas optam por hospedar os dados em múltiplas localidades. Nesse sentido, a ISO/IEC TR 23.186, de 2018, e a ISO 22.095, de 2020, se referem às melhores práticas mercadológicas para implementação de arquiteturas e padrões que subsidiem a uniformização de

terminologias e de requisitos essenciais, de forma a facilitar as tratativas entre provedores de serviços.

Ademais, boas práticas internacionais podem ser utilizadas como norteadoras metodológicas, em razão de sua ampla adoção por outros países e pela independência técnica e acreditação dos padrões internacionais para a concepção de um manual metodológico. Nesse sentido, não se trata somente de ênfase à técnica já reconhecida, mas também do viés jurídico para acreditação e para admissibilidade jurídica de provas digitais.

São exemplos de boas práticas internacionais com os respectivos conteúdos, as citadas a seguir:

- ISO 27037/2012: orientações para a identificação, coleta, aquisição e preservação de evidências forenses digitais. Visa à manutenção da integridade das evidências;
- ISO 27041/2015: orientações sobre como garantir a adequação de métodos investigativos utilizados de acordo com o propósito;
- ISO 27042/2015: diretrizes para análise e interpretação de evidências digitais;
- ISO/IEC 27050/2018-2021: padrão metodológico e procedimental para coleta e investigação de evidência digital;
- BSI 10008/2008: valoração de prova eletrônica e admissibilidade legal de artefatos digitais.

Tais normas abrangem com certa amplitude as boas práticas relativas às investigações sobre crimes cibernéticos, servindo de referência segura justamente por seu reconhecimento. Então, literalmente, deduz-se que, se por um lado a legislação brasileira tem avançado timidamente nos problemas relativos à obtenção de provas digitais, por outro, não se pode dizer que faltam orientações de práticas reconhecidas internacionalmente. Talvez reste reconhecer que, na prática, tal como nos EUA em relação às *Big Techs*, haja resistência em se cumprirem alguns procedimentos, em face do compromisso negocial junto ao cliente de preservação particular dos dados.

4.3 Regulação no cenário brasileiro

A constante e brusca evolução da TI, sempre com novas tecnologias, modificou a “forma coloquial” e particular com que tradicionalmente se manejava o conhecimento. A necessidade de adaptação ao novo paradigma foi incondicional, acarretando conflitos maiores ou menores, que reclamam solução. Por se tratar de conflitos gerais, globais, seus reclames impactaram e continuam a impactar a área jurídica, que, por sua vez, além de também necessitar adaptar-se ao novo em todos os ramos do Direito, deve buscar responder à sociedade. De forma semelhante, no Direito Penal e no Direito Processual Penal, podem ser percebidas, de forma mais preponderante, as inovações promovidas nesse sentido, principalmente no que diz respeito ao uso de dados digitais como prova (ALMAS; GASTAL, 2021, p. 4). Porém, como já dito, os avanços são tímidos frente a voracidade das inovações.

A extensão e a intensidade da utilização das novas tecnologias tornaram a comunicação muito mais eficiente, mas também deixaram os cidadãos mais vulneráveis. Os limites historicamente construídos para a atuação persecutória estatal em muitas situações parecem não mais responder adequadamente às necessidades atuais (FREITAS, 2022, p. 16).

A legislação é taxativa ao estabelecer que tanto o Ministério Público quanto a polícia e outras autoridades, para obterem e se utilizarem, de modo válido, de dados ou outros documentos em investigações, necessitam de autorização judicial específica, concedida apenas mediante a demonstração de indícios de autoria e de provas suficientes de materialidade (FREITAS, 2022, p. 16-17).

Mas quando os dados buscados estão disponibilizados em redes sociais, os requisitos não são suficientemente claros, da mesma forma que não é clara a possibilidade de o Ministério Público ou as autoridades policiais requisitarem dados cadastrais ou de conexão que se encontrem na posse de operadoras telefônicas e de empresas provedoras de Internet. Essas questões são foco de grandes discussões no STF e no STJ, com respostas sem uniformidade e que nem sempre põem em destaque, expressamente, o direito à privacidade (FREITAS, 2022, p. 17).

Nesse sentido, a Quinta Turma do Superior Tribunal de Justiça, no AgInt na Rcl 41.841-RJ, Rel. Ministro Mauro Campbell Marques, por unanimidade, julgado em

08.02.2023, decidiu: “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” (STJ, 2023, p. 34).

Nessa mesma direção, cita-se o desfecho anulatório das referidas operações Satiagraha (2011) e Spoofing (2019) da Polícia Federal, por ilegalidade no procedimento de coleta e de extração de provas digitais. Colacionam-se ainda outros julgados correlatos: RHC n. 78.065SP (STJ); HC n. 517,509/SP (STJ); AgRg no HC n. 499.425/SC (STJ); HC n. 432.896/MG (STJ); RHC n. 67.379/RN (STJ); HC n. 315.220/RS (STJ); RE 680.967; STF, Inq-AgR 2245/MG, Rel. Min. Joaquim Barbosa, DJe 09.11.2007 e HC 106.566/SP.

O exercício do Direito Penal nesse novo paradigma “é uma tarefa que não envolve apenas a análise de crimes virtuais ou crimes cometidos através da Internet. Tampouco se limita a discutir a produção de provas nos meios digitais [...]”. O que há também é a grande necessidade de uma revisão teórica sobre as novas relações entre indivíduo e Estado, de modo a se restabelecerem os marcos jurídicos fundamentais frente à nova realidade. Urge uma regulação da informação que determine a proteção do indivíduo (FREITAS, 2022, p. 17).

Apesar dos avanços presentes no pacote anticrime, que trouxe em seus institutos a cadeia de custódia (conforme já dito), o *codex* pátrio limitou-se a abordar a manutenção de artefatos (*pendriv*es, computadores, discos rígidos, etc.), não adentrando tratativas atinentes a provas totalmente digitais (dados armazenados em plataformas de nuvem computacional, redes sociais e sistemas de armazenamento – Google Drive, Dropbox, etc.).

Como é sabido, as mudanças legislativas no cenário brasileiro são morosas e demandam anos para serem concluídas e levadas à votação pelo parlamento. A título exemplificativo, cita-se a própria atualização do CPP, que durou oito anos até ser finalmente unificada a outros PLs e levada a plenário. Nesse sentido, o uso de mecanismos regulatórios pode suprir o engessamento legal e possibilitar garantias mínimas a serem cumpridas pelas autoridades policiais e pelos provedores de serviços digitais (nuvem computacionais e redes sociais). A finalidade é melhor subsidiar a segurança jurídica dos dados ali coletados e, com isso, garantir o pleno cumprimento de requisitos cientificamente comprovados de segurança: confiabilidade, auditabilidade, integridade, disponibilidade e confidencialidade, não repúdio.

Nesse contexto, cumpre lembrar que o Ministério de Justiça, antes da sanção do novo CPP (2015), publicou o documento “Procedimento Operacional Padrão: Perícia Criminal” (POP), em 2013, cujo terceiro capítulo se volta para a Informática Forense e tem como objetivo “orientar o profissional de perícia da área de informática a realizar exames que envolvam dados contidos em mídias de armazenamento computacional” (MJ, 2013, p. 87). Inclusive, os procedimentos a serem observados acerca da cadeia de custódia são uma tradução literal do documento criado pelo Federal Bureau of Investigation (FBI) norte-americano.

O MJ publicou também a Portaria n. 82, de 16 de julho de 2014, que “Estabelece as Diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígios”, considerando:

- que a cadeia de custódia é fundamental para garantir a idoneidade e a rastreabilidade dos vestígios, com vistas a preservar a confiabilidade e a transparência da produção da prova pericial até a conclusão do processo judicial;

- que a garantia da cadeia de custódia confere aos vestígios certificação de origem e destinação e, consequentemente, atribui à prova pericial resultante de sua análise, credibilidade e robustez suficientes para propiciar sua admissão e permanência no elenco probatório; e a necessidade de instituir, em âmbito nacional, a padronização da cadeia de custódia [...] (MJ/SENASP, 2014, p.289).

Contudo, os documentos brasileiros encontram-se defasados. A título comparativo, cita-se o manual elaborado pelo citado NIST, que dispõe de padrões internacionalmente acreditados, como o NISTIR 8006 e o NIST Cloud Computing Forensic Science Challenges, publicados em agosto de 2020. Também publicou um conjunto de outros documentos normativos nesse mesmo ano, discutindo questões afetas a tecnologias disruptivas, como: cibersegurança, tecnologia 5G, *blockchain* e computação em nuvem em satélite.

Sobre essa temática, Lugo e Rúa (2021) e Vasykov e Khisamova (2019) realizaram extensa abordagem teórica acerca do valor das provas eletrônicas e da importância de envolvimento de um perito especializado em todas as etapas do processo da perícia forense digital (coleta, exame, análise e relatório), conforme aduz a ISO 27037, de 2012.

A propósito, nesse contexto, há alusões à desconfiança processual, segundo a qual "ninguém tem por que acreditar que algo é aquilo que a parte que o apresenta diz que é, simplesmente porque ela assim afirma". Pelo grau de vulnerabilidades implícitas em relação a seu manuseio e à grande probabilidade de erros, exige-se intervenção técnica. Aliás, “com efeito, quando bem compreendidas, as tecnologias digitais devem (ou deveriam) minar nossa confiança sobre a natureza original, genuína e autêntica do que vemos e ouvimos” (FLORIDI, 2018, apud MASSENA, 2023, p. 2).

Inicialmente, definir critérios teóricos para a disposição de limites e de possibilidades nessa área de atuação é importante e urgente no momento em que se vive. O Direito Penal, devido a inúmeros fatores, pode ser considerado um meio “de gestão de riscos sociais, perdendo sua função clássica de *ultima ratio* para ser *prima* ou *sola ratio*”. O ponto mais importante para balizar a atuação estatal passa dos limites para a coleta de dados pessoais para os limites de seu uso após compartilhamento. Entra em discussão aí, em matéria penal, o papel da regulação da privacidade digital frente à proteção de direitos fundamentais (FREITAS, 2022, p. 18).

Em termos gerais, atuações de regulação setorial, realizadas por agências reguladoras ou por Conselhos Nacionais, têm seu fluxo processual de aprovação agilizado. Isso possibilita que resoluções e/ou políticas nacionais sejam adotadas rapidamente pelo mercado e pelo setor regulado. É o caso da Resolução n. 332, de 21 de agosto de 2020, do CNJ, que disciplinou um conjunto de princípios a serem adotados pelo Judiciário em relação ao uso de Inteligência Artificial. Inclusive, adentra questões polêmicas relativas aos direitos fundamentais e à proteção de dados pessoais.

Também é o caso da recente deliberação de uma política de segurança cibernética da Agência Nacional de Energia Elétrica (ANEEL), por meio da Resolução Normativa n. 964, de 14 de dezembro de 2021, que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica (ANEEL, 2021, p. 1). A Resolução a ser adotada pelos agentes do setor de energia elétrica tem como objetivo “aumentar resiliência dos sistemas usados pelo setor de energia elétrica”, com medidas que possam “garantir continuidade dos serviços e segurança de dados críticos” e de definir padrões nacionais para fortalecimento da segurança energética do Brasil. As razões de criação dessa política, segundo essa

Agência, foram: a grande conectividade do sistema elétrico – “[...] cada vez mais estamos conectando os sistemas, as estações são assistidas remotamente, para isso se faz uso de redes lógicas que precisam estar protegidas de ataques cibernéticos" – , o aumento de ataques dos *hackers* e a “falta de uma norma regulamentadora adequada” (SANT’ANA, 2021, p. 4).

Evidentemente, o Direito Penal não se encontra distanciado da regulação das novas tecnologias. “Ao contrário, seu desafio é alcançá-las, visto que as plataformas digitais e as redes têm sido referidas como um espaço propício ao cometimento de crimes”. Ocorre que as exigências desse ramo do Direito quanto às certezas das soluções mostram-se incompatíveis com uma legislação aberta. Com isso, até parece ser inevitável que termine por ficar, de certa forma, sempre em posição de desvantagem frente às novas tecnologias. A legislação, sem flexibilidade, “não tem como deixar de ter caráter *ex post*” (BATISTA; KELLER, 2016, p. 169).

Devido às peculiaridades da prova digital, a ausência de uma identificação segura e que garanta preservação desse dado acarreta o risco iminente de sua manipulação, e é essa inviabilidade de identificar possíveis alterações que ocasiona a quebra da cadeia de custódia da prova e gera patente prejuízo ao réu/investigado, que será impossibilitado de contraditar uma evidência cujas origens e meios de obtenção são desconhecidos. Isso gera, por consequência, a inadmissibilidade da prova digital (BICALHO; MIRANDA, 2023, p. 3).

No contexto judiciário brasileiro, conforme já dito, o CNJ, por meio de Resoluções, busca regular o sistema de justiça, norteando e deliberando quanto a ferramentas e ações a serem mantidas pelos Tribunais de Justiça. Nesse sentido, cita-se a Resolução n. 408, de 18 de agosto de 2021, que “dispõe sobre o recebimento, o armazenamento e o acesso a documentos digitais relativos a autos de processos administrativos e judiciais”. Delibera regramento para a juntada de mídias e de correlatos que porventura não caibam no limite de arquivos a serem anexados aos autos no sistema Processo Judicial Eletrônico (PJE). Contudo, não há regramento específico para cumprimento de cadeia de custódia de evidências digitais e/ou que envolvam dados originários de redes sociais e/ou plataformas digitais em nuvens computacionais.

Pinheiro (2013, p. 282) se refere, por exemplo, à ata notarial, e explica que ela tem serventia para a fixação dos dados cronológicos de sua lavratura, relatando, ainda, o seguinte: “*sites* invadidos; páginas com práticas de fraudes; conteúdo de *e-mails*; análise de conteúdos fechados para assinantes; interação com os sujeitos objeto de monitoramento; prova de fatos caluniosos” e outros dados que devam servir a esclarecimentos.

Porém, há que se levar em conta que a ata notarial, embora seja lavrada por um tabelião, não deixa de ser um documento produzido unilateralmente, com escrutínio do perfil e do dispositivo informático do ofendido. Dessa forma, não possui caráter absoluto e cede diante de prova em contrário, principalmente diante das inúmeras possibilidades de se forjar uma prova virtual (SOUZA, 2021, p. 90).

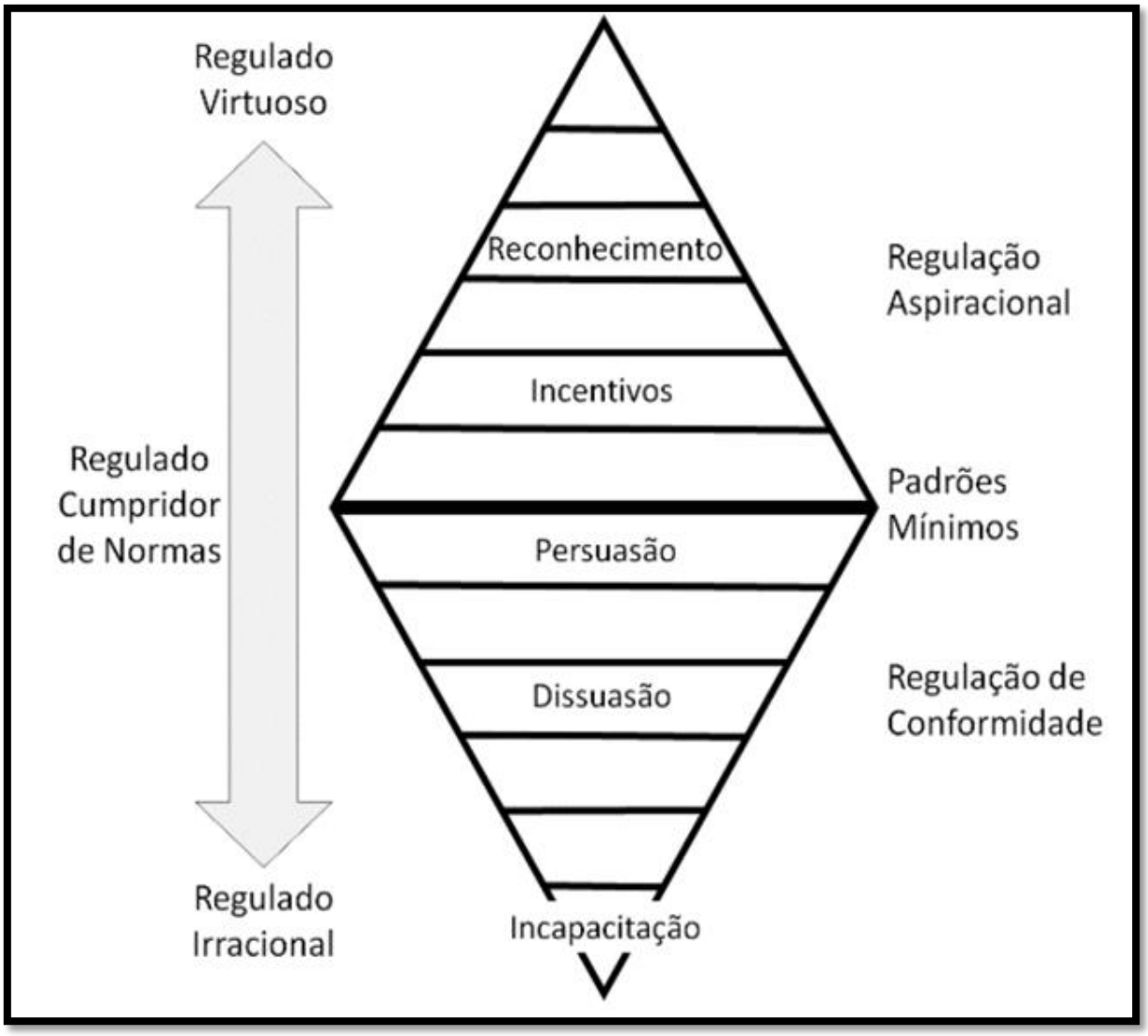
Na esfera privada, soluções tentam mitigar os riscos de nulidade probatória de evidências digitais. Como exemplo, tem-se a ferramenta *on-lin*e de coleta de provas digitais auditáveis denominada *Verifac*t. O objetivo da plataforma é “atender normas forenses e os princípios de coleta e preservação da cadeia de custódia (Lei 13.964/2019), além de possuir um ambiente de registro antifraude que previne a manipulação do conteúdo durante o registro e antes da preservação” (VERIFACT, 2023, p. 1). Foi desenvolvida com a utilização de referenciais à ISO sobre a temática, que já dispõe de acreditação por algumas instituições, bem como a ampla jurisprudência de aceitabilidade. É o que informa o *website* da empresa acerca do assunto).

Entretanto, apesar dos esforços mercadológicos para suprir as lacunas do CPP, principalmente frente à constante e rápida evolução tecnológica, restam desafios de maior complexidade que demandam maior acreditação, tais como evidências digitais mantidas em ambiente virtual, com múltiplas jurisdições, comumente encontradas em plataformas digitais de nuvem computacional.

A atividade regulatória estatal tem como foco o interesse público, para o qual deve ser orientada. Porém, não pode ignorar a realidade setorial e as respectivas dinâmicas, para evitar que a regulação seja incompetente, ineficaz ou insuficiente a ponto de não promover mudanças no comportamento dos agentes (TRINDADE, 2019, p. 56).

No cenário pátrio, a LGPD, entre outros normativos, destacou-se pela inserção de mecanismos regulatórios junto à Autoridade Nacional de Proteção de Dados (ANPD). Tal fato possibilita implementar a estrutura do diamante regulatório apresentado por Kolieb (2015), para aplicações de sanções em casos de vazamentos de dados pessoais de cidadãos brasileiros, conforme ilustrado na Figura 2 a seguir.

Figura 2 - Diamante Regulatório



Fonte: Kolieb (2015, apud CARDOSO, 2021, p. 149)

Kolieb (2015, apud CARDOSO, 2021, p. 149) atualizou a abordagem piramidal de Ayres e Braithwaite (1992), acrescentando o que considerou tratar-se de uma “evolução natural”, ou seja, esse diamante regulatório. Ele aprimorou aquela abordagem e a atualizou com a oferta de outra dimensão: a recompensa. A conformidade não é a “linha de chegada”, mas um caminho para uma regulação de

comportamentos que seja virtuosa, porque aprimorada; um meio.

No contexto da LGPD, os órgãos e instituições passíveis de atendimento à citada legislação devem atender critérios mínimos de proteção aos dados que coletam e armazenam, de forma a garantir minimamente os critérios de segurança dispostos nos princípios segurança por *design* e privacidade por padrão. Esses critérios têm suas exigências aumentadas quando os dados armazenados são de maior criticidade, como no caso de dados pessoais sensíveis. O objetivo é mitigar vazamentos e, assim, proteger o cidadão brasileiro de não ter seus dados expostos e/ou utilizados por perpetradores.

Nessa perspectiva, apesar de não existirem garantias para se obter segurança em sua integralidade, os esforços envidados e documentados por empresa passível de inspeção por órgãos controladores (Tribunal de Contas da União, Conselho Nacional do Ministério Público, Conselho Nacional de Justiça e Ministério Público em geral, entre outros) são considerados quando da aplicação de sanções nos casos de vazamentos de dados pessoais pela empresa. Também os critérios mínimos de privacidade e de segurança necessários para a governança de dados, se atendidos, são recompensados por meio de indicadores de desempenho nacionais. Ou seja: no centro da pirâmide, encontram-se as empresas que atendem aos padrões mínimos exigidos pela legislação; no topo, as empresas que superam os padrões e dispõem de modelos de maturidade e governança avançados (reconhecimento); na base, encontram-se as que não atenderam ao disposto legal e serão penalizadas com maior rigor por vazamento de informações pessoais.

4.4 Regulação para coleta e armazenamento de evidências digitais

O mercado, tal como se conhece hoje, representa um “produto normativo, protegido por direitos de propriedade, de igualdade e de liberdade”, significando que as atividades setoriais de relevância constituem produtos da regulação jurídica. Nessa perspectiva, os movimentos desregulatórios ocorridos não representaram qualquer afastamento do Estado de seu poder de regular; foram apenas reformas na regulação que, diante do momento temporal de necessidades urgentes, dispensaram a grande parte da intervenção estatal e, assim mesmo, em algumas frentes (BALDWIN *et al*., 2013, apud CARDOSO, 2021, p. 167).

O Brasil é pioneiro no uso de aspectos regulatórios e legiferantes em diversos cenários, a exemplo dos citados MCI, de 2010, da LGPD, de 2018, e da recente Resolução Normativa n. 964/2021 da ANEEL, que fixa um conteúdo mínimo a ser adotado pelos agentes do setor elétrico para garantir suas informações, sua estrutura tecnológica e a privacidade dos dados de seus clientes.

Nesse contexto, a exemplo da recente intenção de regulamentação de uso de nuvem computacional pelos Estados-membros da UE, com o Cloud Act e a adoção de regramento para solicitações e coletas de evidências digitais, há possibilidades de acreditação de uma Resolução normativa por parte do CNJ. A finalidade é instituir regras e procedimentos a serem adotados pelos operadores do Direito e peritos forenses digitais, visando garantir o pleno cumprimento das melhores práticas na coleta, no armazenamento e na análise de evidências digitais em ambientes de nuvem computacional. Tais práticas poderiam, inclusive, facilitar a tramitação de MLAT entre os países, bem como possibilitar, ao magistrado, maior facilidade na validação de requisitos mínimos que devem ser verificados para a plena garantia da cadeia de custódia de evidências digitais.

Mas também deve-se destacar que autorregulações exclusivas por agentes privados tem limitações, a exemplo das realizadas pelas *Big Techs* (já citadas). Embora a autorregulação tenha um caráter geral de implementação, nem todos os agentes são obrigados a tal adesão e até podem requerer incentivos com altos custos para participar. Grupos pouco articulados, como empresas menores, consumidores e a sociedade em geral podem ficar sem proteção ou mal protegidos diante de regras autorreguladas por grupos dominantes. Ainda se verificam dificuldades de controle de agentes mal-intencionados ou dissidentes. Por último, autorregulações ainda estão sujeitas a regras cujo volume nem sempre acoberte todas as situações (BALDWIN *et al*., 2013, apud CARDOSO, 2021, p. 167).

Recentes teorias regulatórias não consideram algum relaxamento, e sim propõem uma inteligência regulatória maior, inclusive considerando, com base em correntes teóricas distintas, uma intervenção estatal ponderada com “espaços de autonomia controlada do regulado” (CARDOSO, 2021, p. 167).

Como exemplo**,** cita-se a recente decisão do ministro Alexandre de Moraes no Inquérito 4933, instaurado para apurar a atuação de diretores do Google e do Telegram no Brasil em suposta campanha contra o PL n. 2.630/2020, conhecido como

“PL das *Fake News*”. “O motivo foi o descumprimento de decisões reiteradas do STF envolvendo as contas de usuários [...] e o não atendimento ao convite feito pelo Tribunal Superior Eleitoral (TSE) para coibir a disseminação de notícias fraudulentas” (BRASIL, 2023, p. 3). Embora não seja de interesse do Estado afetar diretamente o funcionamento de aplicativos e empresas no âmbito brasileiro, há necessidade de as empresas atenderem à legislação brasileira ao ofertarem serviços direcionados ao público nacional.

Os regulados têm motivações diferentes e, por isso, só uma adequada estrutura regulatória, fixada na dependência mútua da persuasão com a punição e embasada em estratégias regulatórias de retaliação equivalentes, poderia, de um lado, ter capacidade de resposta proporcional às violações e, de outro, reconhecer os esforços dos regulados. O principal pressuposto dessa dependência mútua é o aproveitamento do espaço de influência recíproca e de interação para ampliar a efetividade da regulação, com o voluntário cumprimento das normas e concomitante redução das resistências à conformidade (ARANHA, 2019, apud CARDOSO, 2021, p. 168-169).

Embora tenha legitimidade para a imposição de regras, o Estado não tem noção minuciosa das habilidades nem das limitações da administração privada. Por isso, regras criadas por agentes públicos nem sempre conseguem otimizar competências ou reduzir deficiências. A cooperação da esfera privada está no fato de o particular ter condições de melhor entender o que fazer para obter o desejado, indo além, inclusive, da conformidade. Então, desde que internalizados os compromissos da regulação, a fiscalização do regulado se torna ostensiva e profunda, além de contínua, bem mais do que a fiscalização feita por agentes públicos, aumentando-se a efetividade das estratégias (ARANHA, 2019, apud CARDOSO, 2021, p. 169).

O autor ainda destaca que esse tipo de regulação, chamada de responsiva, não desconsidera nem exclui o controle e o comando, e sim assimila seus princípios, refutando a completa desregulação.

4.5 Requisitos mínimos para acreditação de evidências digitais no direito comparado (EUA X BRASIL)

De acordo com Martini (2015, p. 11), a experiência do sistema judiciário dos EUA é diferente da experiência brasileira no que diz respeito aos controles das provas periciais. Lá, provas científicas são produzidas com o depoimento de uma testemunha detentora de conhecimento especializado. “Nesse contexto, o testemunho do perito difere do depoimento prestado por uma testemunha convencional, pois o primeiro toma conhecimento dos fatos da causa posteriormente”, aplicando a eles a técnica científica, com vistas a alcançar resultados que ajudem o juiz a solucionar o caso. “Um ponto de preocupação da justiça americana era a parcialidade do perito, pois o perito é indicado e remunerado pelas partes para prestar o depoimento”.

Nesse sentido, a partir do caso Frye, decidido pela Court of Appeals of District of Columbia em 1923, foi adotado um critério de aceitação geral, pelo qual apenas se aceitavam testemunhos técnicos daqueles cuja ciência tivesse aceitação geral na comunidade científica. “Esse precedente perdurou por muitos anos e foi amplamente aplicado nas Cortes norte americanas” (MARTINI, 2015, p. 11).

Contudo, em 1975, promulgaram-se as Federal Rules of Evidence (FRE), com a finalidade de a temática das provas nos casos federais. Nenhuma menção houve ao caso Frye, gerando dúvidas se ele ainda era referência ou fora superado pela nova norma. Tal dúvida só foi dirimida em 1993, por ocasião do caso Daubert, quando a Suprema Corte reconheceu que o princípio do caso Frye era incompatível com os as regras 401 e 702 da FRE. Surgiu daí o princípio de Daubert (MARTINI, 2015, p. 12).

A Suprema Corte reconheceu a necessidade de associar novos critérios à aceitação geral, em um rol de fatores não taxativos de apreciação da confiabilidade. Quatro critérios de admissão da prova testemunhal científica foram então adotados nas Cortes federais dos EUA: “I) possibilidade de teste voltada para a falsificação da teoria ou método; II) publicação e submissão da teoria ao chamado processo de revisão por pares; III) indicação do percentual de erro; IV) aceitação geral da teoria ou método entre os estudiosos da área do conhecimento” (MARTINI, 2015, p. 12).

Na lição de Denis Andrade Sampaio Junior (2021, p.123-124), extrai-se que o princípio de Daubert tem como premissa o entendimento de que “a crença da verdade

científica deve ser sopesada por critérios específicos e racionais para o seu valor judicial". Assim, o nível de validade e de comprovação da prova científica "deve ser retratado a partir de alguns métodos específicos, não sendo crível o seu valor absoluto, bem como o seu confronto com o sistema da prova livre para elevar um conhecimento geral". O reconhecimento do valor da prova produzida e sua valoração devem acompanhar um padrão específico, a fim de aferir, com garantia, a verdade "científica" e o critério de validade, para produzirem efeito nas decisões das questões de fato.

Pode-se inferir que, com o passar dos anos e o maior quantitativo de situações que permeiam a necessidade de valoração e acreditação de evidências digitais, maior é a maturidade das decisões e pesquisas científicas realizadas com o fito de consolidar princípios norteadores para atendimento do sistema judiciário.

A propósito, nesse sentido, na jurisprudência brasileira, não se identificam pronunciamentos, à semelhança dos fatos referidos dos EUA, que indiquem "a necessidade cogente de padrões técnicos para a admissibilidade de prova científica no processo". Inclusive, até são incipientes os debates relativos à aplicação de critérios com propósitos semelhantes ao padrão Daubert para provas periciais no sistema processual. Raros julgados de tribunais trazem alguma referência a esse padrão, demonstrando que é incipiente o debate sobre o assunto, bem como não é comum a análise do juiz sobre a metodologia usada por peritos em laudos periciais no CPP (MALTA *et al*., p. 2023, p. 200).

No decurso da pesquisa, foi possível identificar importante artefato criado pela organização de pesquisa sem fins lucrativos, apartidária, presente nos continentes americano, europeu e australiano, intitulada RAND, que, dentre suas linhas de atuação, tem como objetivo o desenvolvimento de soluções para mitigar a problemática de valoração de prova digital, frente aos desafios de políticas públicas, em parceria com instituições governamentais norte-americanas.

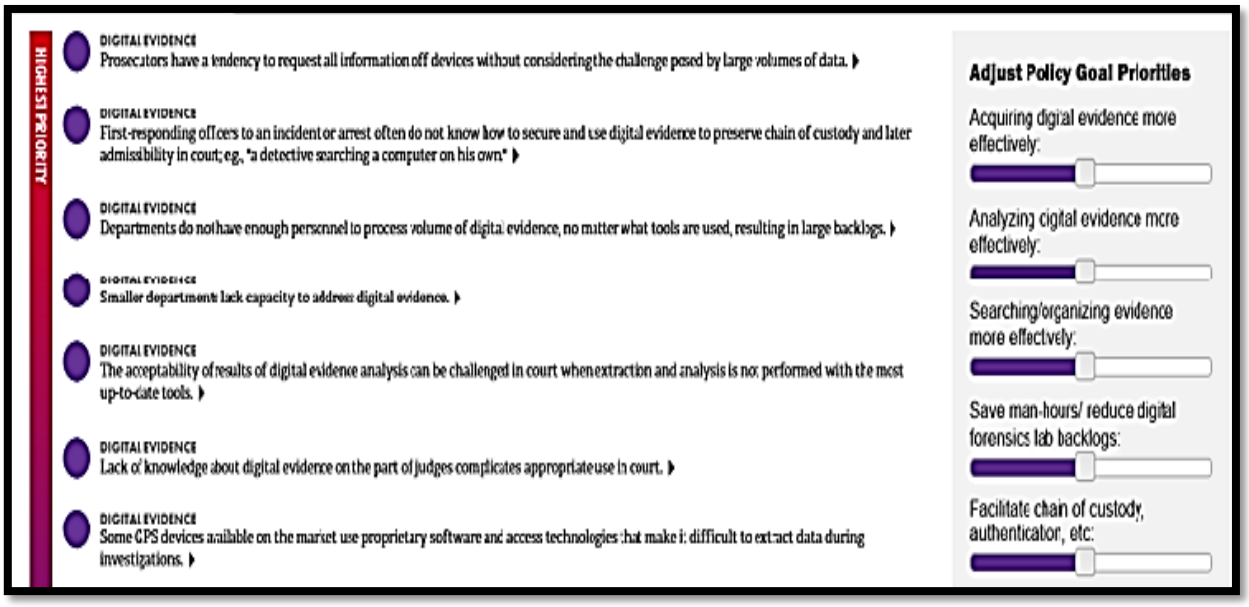
A ferramenta, desenvolvida com fundamentos e premissas na legislação norte-americana, possibilita apoiar os operadores do Direito e peritos forenses na utilização do método Delphi, também desenvolvido pela RAND na década de 1950, amplamente conhecido e cientificado para soluções de problemáticas complexas, na valoração da prova digital por meio de sistema *on-line*. De acordo com os dados informados e com os objetivos a serem alcançados, o usuário é informado sobre necessidades e

requisitos mínimos a serem evidenciados no laudo pericial e/ou, até mesmo, na cadeia de custódia da evidência digital (VERMEER *et al*., 2018, p. 27):

> A ferramenta [...] permite que você veja como as prioridades de diferentes inovações para melhorar a coleta e o uso de evidências digitais pelas agências de justiça criminal mudam quando um peso diferente é dado aos objetivos políticos individuais. O ponto de partida são as classificações desenvolvidas no workshop de evidências digitais do Instituto Nacional de Justiça (NIJ) [...] de 2014. Usando as barras deslizantes para inserir quais metas são mais importantes [...] com base em [...] preferências políticas (à esquerda está a menor importância relativa, a direita é mais alta), as necessidades de evidências digitais serão redefinidas [...] com as mais bem classificadas aparecendo no topo (RAND, 2023, p. 3).

Apenas para ilustrar a dinâmica da ferramenta, que distingue necessidades de alta e de baixa prioridade, no Quadro 3 abaixo, veem-se exemplos de necessidades específicas de evidência digital de alta prioridade, associadas a cada problema.

Quadro 3 - Tela da Ferramenta Interative Tool para Ranqueamento de Evidências Digitais



Fonte: RAND, 2023

Da verificação do exemplo parcial do Quadro 3, pode-se inferir a amplitude da ferramenta desenvolvida, a qual, de acordo com a prioridade, os objetivos e o tipo de evidência digital, dispõe ao usuário um conjunto de necessidades a serem pontuadas

para atender critérios mínimos de admissibilidade da evidência no contexto judicial norte-americano.

Nesse sentido, considerando o escopo desta pesquisa, vislumbram-se adequações da metodologia supramencionada para regular requisitos minimamente aceitáveis para admissibilidade e valoração de provas digitais. Tais requisitos podem se enquadrar tanto nas orientações das ISOs, mencionadas anteriormente, quanto aos modelos regulatórios também apresentados. A finalidade é possibilitar a acreditação de todo o processo tanto no âmbito público (envolvimento de peritos e de operadores do Direito especializados na temática) quanto no acadêmico e no mercadológico (empresas de tecnologia que hospedam e/ou fornecem soluções em ambiente de nuvem computacional e/ou redes sociais para o Brasil e, portanto, de atendimento à legislação brasileira), assim como no âmbito dos representantes da sociedade civil, os quais também podem contribuir para a definição de critérios e de métodos a serem usados.

A regulação aqui proposta traz como diferencial a flexibilidade de sua adaptação, podendo ser definida tanto pela segunda instância de um Tribunal de Justiça, aplicando-se jurisdição à qual ele pertença, quanto por tribunais superiores, Conselho Superiores e/ou Ministério da Justiça, de acordo com as referências aos padrões operacionais de coleta e de extração de provas atualmente vigentes (e desatualizados), com a referida Portaria n. 82/2014 e com o também citado “Procedimento Operacional Padrão” (POP), que datam de 2013 e de 2014 e não refletem, na atualidade, a necessidade e a evolução tecnológica atuais.

CONCLUSÃO

A tecnologia deve ser compreendida com base em suas consequências concretas nas relações sociais, sem que se perca de vista o fato de que ela é um produto das relações sociais. Como tal, é construída segundo determinados interesses com vistas a alcançar objetivos especificados que, muitas vezes, têm pouca relação com as “maravilhas” prometidas por seus defensores. Portanto, a análise das relações entre tecnologia e sociedade não pode ser feita acriticamente, já que, apesar dos Projetos de Lei, a regulação das tratativas e o tratamento que o Direito dá a elas deve se pautar por dados concretos decorrentes de sua aplicação, e não a partir de suas possibilidades.

O campo da evidência digital é novo e, como decorre da evolução da tecnologia que instalou um novo paradigma – aproximação de interesses independentemente da geografia; simplificação cada vez maior de rotinas sociais e reorganização da vida empresarial, entre outras –, acompanha sua expansão em latitude e longitude. Porém, faltam a essas medidas, metafóricas ou reais, coordenadas que permitam não a localização de evidências digitais, mas o acesso a elas no caso de crimes digitais.

Potencialmente, a evidência digital constitui uma importante fonte de informação, que pode auxiliar os operadores do Direito na solução e no deslinde de crimes digitais. A forma como a tecnologia intervém nas atividades cotidianas globais, por si só, possibilita estimar o potencial de dados manuseados diariamente, dados esses que aumentam exponencialmente à medida que a dinâmica dessas atividades se estende, ampliando simultaneamente seus campos de ação em benefícios e problemas.

Diante disso, verificou-se que tais informações, via evidências digitais, apresentam grande valor probatório na esfera processual penal, podendo ser utilizadas como prova que proporciona a aplicação de princípios constitucionais, como o contraditório e a ampla defesa, e promove o convencimento do julgador.

Entretanto, para constituir uma prova, faz-se imprescindível que o dado digital, como fonte probatória, passe por controles epistêmicos que garantam sua integralidade e a respectiva confiabilidade. É nessa senda que se encontra a cadeia de custódia da prova digital, como meio de garantir a preservação da fidedignidade

da prova por meio do emprego de procedimentos e de etapas próprias de acordo com suas particularidades.

Por longo período de tempo, não houve regulamentação da cadeia de custódia no ordenamento jurídico brasileiro, o que gerava dúvidas acerca da confiabilidade e da acreditação do material probatório e prejudicava a possibilidade de discernimento em relação às provas ilícitas em geral e a verificação das razões que levavam à respectiva contaminação. Com o sancionamento da Lei 13.964/2019, que dispõe sobre o aperfeiçoamento da legislação penal e processual penal, passou-se a ter, no CPP, o procedimento da cadeia de custódia.

Contudo, dada a morosidade do processo legislativo para aprovação de legislações complexas, a nova lei já nasceu defasada, com lacunas de atendimento às novas tecnologias e a seus efeitos nefastos, também em constante evolução. Com isso, não se pôde efetivamente cumprir o disposto em relação à cadeia de custódia de dados integralmente digitais.

É no ponto entre a defasagem no uso da cadeia de custódia e a intensidade com a qual os dados digitais vêm sendo utilizados como fontes probatórias que se faz de extrema urgência a necessidade de regulamentação da cadeia de custódia das provas digitais, tornando obrigatória a aplicação do instituto.

Apesar da iniciativa de Projetos de Leis, como o PL n. 4939/2020, que promove a inclusão da cadeia de custódia das provas digitais no CPP, salienta-se que o conteúdo do texto sugerido carece de elementos que solidifiquem as etapas desse instituto, abarcando conceitos e procedimentos a serem executados.

No decurso deste trabalho, propôs-se discutir o uso do instituto da regulação para por meio da própria esfera administrativa, possa se regulamentar padrões mínimos de aceitabilidade para garantir a cadeia de custódia, a coleta e armazenamento de dados integralmente digitais, garantindo que as provas a serem valoradas e posteriormente admitidas no processo penal estejam resguardadas de contaminação e ilicitude.

Nesse sentido, buscou-se analisar como o direito comparado, principalmente o norte-americano e o europeu, tem enfrentado a ubiquidade tecnológica alijado no crescimento de ocorrências de crimes no mundo cibernético para acreditar juridicamente procedimentos técnicos e metodologias científicas passíveis de

aplicação pelos operadores de direito nessa nova temática.

A pesquisa conclui que a utilização da regulação pode vir a ser um grande diferencial, em razão da maior flexibilidade de ajustes e de melhorias perante aos agentes de regulação, possibilitando maior participação das empresas *Big Techs*, da academia, de especialistas do mercado e da própria sociedade civil na propositura de padrões mínimos a serem considerados pelo magistrado como ferramenta de apoio decisório, com vistas a nortear a pontuação de cumprimento de requisitos, a fim de se garantir pontuação mínima para acreditação e valoração de provas digitais.

Ademais, de modo complementar ao objetivo da pesquisa, o trabalho apresenta de forma condensada o estado da arte dos principais padrões internacionais acreditados pelo mercado na disciplina ciência forense computacional, bem como normativas norte-americanas e a recente regulação da União Europeia para a temática, sugerindo a adequação de ferramenta desenvolvida pela organização de pesquisa RAND para valoração de provas digitais, como alternativa para garantir o que pode ser solicitado de acordo com a tecnologia aplicada, quais riscos e particularidades envolvidos e quais padrões e metodologias são acreditados para determinado tipo de prova digital.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR 27.001:2013**. Sistema de Gestão de Segurança da Informação (SGSI). Rio de Janeiro, 2013.

ABNT. Associação Brasileira de Normas Técnicas. **NBR 27.037:2012**. Tecnologia da informação. Técnicas de segurança. Diretrizes para identificação, coleta, aquisição e preservação de evidência digital: Referências. Rio de Janeiro, 2013a.

ABREU, J. S. Conflitos de jurisdição por provas digitais, reforma da cooperação judiciária internacional e a experiência brasileira. **Revista de Informação Legislativa**, v. 55, n. 220, p. 233-257, out./dez. 2018. Disponível em: http://www12.senado.leg.br/ril/edicoes/55/220/ril_v55_n220_p233. Acesso em: 01 maio 2023.

ALMAS, Amanda Costa das; GASTAL, Mariana. **A aplicabilidade da cadeia de custódia em dados digitais utilizados como prova no processo penal brasileiro**. 2020. Monografia (Aperfeiçoamento/Especialização em Laboratório) – Instituto Brasileiro de Ciências Criminais, Porto Alegre, 2020. Disponível em: www.ibccrim.org.br. Acesso em: 12 ago. 2023.

AMAZON. **Law enforcement information requests**. Disponível em: https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF. Acesso em: 20 ago. 2023.

ANEEL. Agência Nacional de Energia Elétrica. **Resolução ANEEL n. 964/2021, de 14 de dezembro de 2021**. Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica. Disponível em: https://www2.aneel.gov.br/cedoc/ren2021964.html. Acesso em: 6 maio 2023.

ANULAÇÃO da Satiagraha e condenação de Protógenes transitam em julgado. **Consultor Jurídico**, 19 de agosto de 2015. Disponível em: https://www.conjur.com.br/2015-ago-19/anulacao-satiagraha-condenacao-protogenes-sao-definitivas. Acesso em: 01 maio 2022.

ARANHA, Marcio Iorio. **Manual de direito regulatório**: fundamentos de direito regulatório. 8. ed. London: Laccademia, 2023.

ARRUDA, E. N. **Identificando o grau de dependência da adesão à computação em nuvem**. 2013. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2013. Disponível em: https://www.ufpe.br/documents/39830/1359036/241_EduardoArruda/1e79f5bf-1bb4-4070-8ea1-9308f93a066d. Acesso em: 22 jul. 2023.

AWS. Amazon. **Lei de esclarecimento do uso legítimo de dados no exterior (CLOUD)**: como a lei cloud afeta a AWS. 2018. Disponível em: https://aws.amazon.com/pt/compliance/cloud-act/#:~:text=Como%20a%20Lei%20CLOUD%20afeta,autoridades%20policiais%20dos%20Estados%20Unidos. Acesso em: 20 ago. 2023.

BAPTISTA, P.; KELLER, C. I. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. **Revista de Direito Administrativo**, v. 273, p. 123-163, set./dez. 2016. Disponível em: https://periodicos.fgv.br/rda/article/view/66659. Acesso em: 22 set. 2023.

BARLOW, John P. **Declaração de independência do ciberespaço**. Davos, 1996. Disponível em: https://www.eff.org/pt-br/cyberspace-independence. Acesso em: 30 abr. 2023.

BARRETO, A. G. Preservação da evidência eletrônica: desafio à polícia judiciária. **Revista Eletrônica Direito & TI**, v. 1, n. 4, 2016. Disponível em: https://direitoeti.com.br/direitoeti/article/view/70/68. Acesso em: 21 set 2023.

BARRETO, A. G; BRASIL, B S. **Manual de Investigação cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016.

BERBERI, Marco Antonio Lima; HANTHORNE, Bruna de Oliveira Cordeiro. Aspectos controvertidos no uso da prova digital no ordenamento jurídico brasileiro. **International Journal of Digital Law**, ano 2, n. 2, p. 137-165, 2021. Disponível em: https://journal.nuped.com.br/index.php/revista/article/view/hanthorne2021/229. Acesso em: 26 ago. 2023.

BICALHO, Camila Fernandes; MIRANDA, Felipe A. Ribeiro. O caso Anderson Torres e a admissão da prova digital no processo penal. **Consultor Jurídico**, 10 de fevereiro de 2023. Disponível em: https://www.conjur.com.br/2023-fev-10/bicalho-miranda-admissao-prova-digital-processo-penal. Acesso em: 10 fev. 2023.

BRASIL. Superior Tribunal de Justiça. **Rcl 41.841-RJ – AgInt**. (Quinta Turma). Relator: Ministro Mauro Campbell Marques, 08 de fevereiro de 2023.

BRASIL. Supremo Tribunal Federal. **ADC n. 12-DF**. Relator: Ministro Carlos Britto, 20 de agosto de 2008. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=606840. Acesso em: 12 maio 2023.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus 222.141**. Relator: Ministro Ricardo Lewandowski. 14 de dezembro de 2022. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/HC222141.pdf. Acesso em: 10 jun. 2023.

BRASIL. Supremo Tribunal Federal. **Inq 4933**. Relator: Ministro Alexandre de Moraes, 12 de maio de 2023. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/DecisoInquerito4933.pdf. Acesso em: 10 jun. 2023

BUDAPESTE. **Convenção sobre o Cibercrime (Convenção de Budapeste)**. 2001. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 01 maio 2023.

CAMPOS, R. **Metamorfoses do direito global**: sobre a interação entre direito, tempo e tecnologia. São Paulo: Conta Corrente, 2022.

CARDOSO, Fernando Roriz Marques. **CGU além do comando e controle**: uma comparação com a regulação responsiva. **Revista de Direito Setorial e Regulatório**, v. 7, n. 1, p. 150-193, maio/jun. 2021.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999. v. 1.

CASTELLS, Manuel. **Fim do milênio**. 4. ed. Tradução Klaus Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007.

CASTRO, A. L. C. Crimes cibernéticos e óbices ao cumprimento do Acordo de Cooperação Internacional (MLAT) com base nos *standards* de causa provável e liberdade de expressão do Direito estadunidense. **Revista do Ministério Público do Estado do Rio de Janeiro**, n. 76, abr./jun. 2020. Disponível em: https://www.mprj.mp.br/documents/20184/1904621/Ana_Lara_Camargo_de_Castro.pdf. Acesso em: 01 maio 2023.

CD. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 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: www.camara.gov.br. Acesso em: 23 maio 2023.

CD. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 4291/2020**a. Altera o Decreto-Lei n. 3.689, de 3 de outubro de 1941 (Código de Processo Penal) a fim de dispor sobre a custódia dos elementos digitais de prova. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1924108&filename=PL%204291/2020. Acesso em: 23 maio 2023.

CD. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 4939/2020**. Dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências. Disponível em: https:// www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2264367. Acesso em: 30 abr. 2023.

CD. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 8045/2010**. Código de Processo Penal.
Disponível em: https:// www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263. Acesso em: 2 maio 2023.

CERQUEIRA, Tarcisio Queiroz. O direito do ciberespaço. **Jus Navigandi**, 01 de novembro de 1999. Disponível em: https://jus.com.br/artigos/1774/o-direito-do-ciberespaco/2. Acesso em: 20 ago. 2023.

CIN/UFPE. Centro de Informática da Universidade Federal de Pernambuco. **Internet conceitos e serviços**. Disponível em: https://www.cin.ufpe.br/~flash/resultados/cursos/taais/1997-2/Internet/internet.html. Acesso em: 19 ago. 2023.

CNJ. Conselho Nacional de Justiça. **História do CNJ**. Disponível em: https://www.cnj.jus.br/sobre-o-cnj/cnj-18-anos/. Acesso em: 20 ago. 2023.CNJ. Conselho Nacional de Justiça. **Resolução n. 408**, de 18 de agosto de 2021. Dispõe sobre o recebimento, o armazenamento e o acesso a documentos digitais relativos a

autos de processos administrativos e judiciais. Disponível em: http://atos.cnj.jus.br/files/original13325420210820611faf0696a9b.pdf. Acesso em: 23 ago. 2023.

COMENALE, Felipe Becari. O direito na sociedade da informação. **Jus**, 27 de março de 2018. Disponível em: https://jus.com.br/artigos/65068/o-direito-na-sociedade-da-informacao. Acesso em: 29 ago. 2023.

COSTA-NETO, João; TRINDADE, Bruno Rodrigues. A relevância da perícia para a atuação dos operadores do Direito. *In*: COSTA-NETO, João; AMATO, Lucas Fucci; BUSTAMANTE, Thomas (org.) **A prova**: ensaio em homenagem a Frederick Schauer. Rio de Janeiro: Lumen Juris. 2023. v. III. p. 205-228. (Coleção Fundamentos do Direito)

DIAS, Maria Tereza Fonseca; SILVA, Samira Souza. A crise da lei no estado democrático de direito e o papel da legística no restabelecimento da racionalidade jurídica. **Revista Brasileira de Filosofia do Direito**, v. 3, n. 2, p. 36-56, 2017.

EU. European Comission. E-evidence - cross-border access to electronic evidence. **Projeto E-evidence**. 2022. Disponível em: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en. Acesso em: 10 out. 2023.

EU. European Union. Conselho. **Proposta de regulamento do Parlamento Europeu e do Conselho relativa às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal 2018/0108 (COD**). Disponível em: https://data.consilium.europa.eu/doc/document/ST-10312-2023-INIT/pt/pdf. Acesso em: 21 ago. 2023.

EU. European Union. Parlamento. **Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho**, de 12 de julho de 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32023L1544. Acesso em: 11 ago. 2023.

EUA. U.S Departament of Justice. **Cloud Act**. Disponível em: https://www.justice.gov/dag/cloudact. Acesso em: 01 maio 2023.

EUR-LEX. **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrônicas em matéria penal**. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri =CELEX:52018PC0225&from=PT. Acesso em: 01 maio 2023.

FELICIANO, Guilherme Guimarães. Informática e criminalidade - parte I: lineamentos e definições. **Boletim do Instituto Pedro Pimentel**, São Paulo, v. 13, n. 2, 2000.

FERNANDES, Márcio Aurélio de Souza; OLIVEIRA, Fernando G.; FERRAZ, Felipe Silva; SILVA, Daniel Alves; CANEDO, Edna Dias; SOUSA JR., Rafael Timóteo. Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da computação em nuvem. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. Extra 42, fev. 2021, p. 374-385. Disponível em: https:pp.eee.unb.br. Acesso em: 28 ago. 2023.

FERREIRA FILHO, M; FERREIRA, D. Legalidade e regulação na constituição federal de 1988. **Revista de Direito Administrativo e Gestão Pública**, Curitiba, v. 2 n. 2, p. 124-144, jul./dez. 2016. Disponível em: https://indexlaw.org/index.php/rdagp/article/view/1301/1727. Acesso em: 5 out. 2023.

FONSECA, Marcos De Lucca; GENNARINI, Juliana Caramigo. A adesão do Brasil à Convenção de Budapeste e os impactos para a produção de provas digitais. **Revista de Direito Penal e Processo Penal**, v. 4, n. 1, p. 55-70, jan./jun. 2022. Disponível em: https://revistas.
anchieta.br/index.php/DireitoPenalProcessoPenal/article/view/1887/1652. Acesso em: 25 ago. 2023.

FRANÇA, Rubens Limongi. **Hermenêutica jurídica**. 8. ed. São Paulo: Revista dos Tribunais, 2008.

FREITAS, Marcio Luiz Coelho de. **Privacidade no direito penal e o dilema da vigilância na era digital**: a regulação da internet como instrumento de tutela de direitos fundamentais. 2022. 236 f. Tese (Doutorado em Direito) – Universidade de Brasília, Brasília, 2022. Disponível em: http://www.realp.unb.br/jspui/handle/10482/44262. Acesso em: 21 out. 2023.

GALVIS LUGO, A. F.; BUSTAMANTE RÚA, M. M. La valoración de la prueba electrónica y de la prueba documental en el ámbito civil, diferencias e implicaciones. **The Law, State and Telecommunications Review**, v. 13, n. 2, p. 155-197, October 2021. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/37266. Acesso em: 21 set. 2023.

GARTNER. **Products in cloud infrastructure and platform services (transitioning to strategic cloud platform services) market**. Disponível em: https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform-services. Acesso em: 10 set. 2023.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. **Revista de Doutrina da 4ª Região**, n. 55, ago. 2013. Disponível em: https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 17 ago. 2023.

GOODISON, Sean E.; DAVIS, Robert C.; JACKSON, Brian A. Digital evidence and the U.S. criminal justice system: identifying technology and other needs to more effectively acquire and utilize digital evidence. **Priority Criminal Justice Needs Initiative**, 2015. Disponível em: https://www. ojp.gov/pdffiles1/nij/grants/248770.pdf. Acesso em: 20 maio 2023.

ITAENU, Oliver. **Internet et le droit**: aspects juridiques du commerce életronique. Paris: Eyrolles, 1996.

JESUS, D; MILAGRE, J A. **Manual prático de crimes informáticos**. São Paulo: Saraiva, 2016.

KELSEN, Hans. **Teoria pura do direito**. 6. ed. São Paulo: Martins Fontes, 1998.

KING, Lawrence. **LGPD e GDPR**: quais as diferenças e semelhanças? 2020. Disponível em: https://www.nextlawacademy.com.br/blog/lgpd-e-gdpr-quais-as-diferencas-e-semelhanças. Acesso em: 21 ago. 2023.

KNOPFELMACHER, M; CAVALCANTI, F L. Operação Spoofing: prova ilícita e imprestável. **Folha de São Paulo**, 4 de fevereiro de 2021. Disponível em: https://www1.folha.uol.com.br/opiniao/2021/02/operacao-spoofing-prova-ilicita-e-imprestavel.shtml. Acesso em: 30 abr. 2023.

LAI, S.; MOURÃO, P. B. A prova digital no projeto para o novo CPP: em busca do necessário equilíbrio. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-prova-digital-no-projeto-para-o-novo-cpp-em-busca-do-necessario-equilibrio-26052021. **Jota**, 26 de maio de 2021. Acesso em: 29 abr. 2023.

LAVAREDA, Antonio. Big techs ameaçam autonomia dos estados. **Consultor Jurídico**, 19 de abril de 2022. Disponível em: https://www.conjur.com.br/2022-abr-19/antonio-lavareda-big-techs-ameacam-autonomia-estados. Acesso em: 20 ago. 2023.

LEMOS, Diego Fontenele; CAVALCANTE, Larissa Homsi; MOTA, Rafael Gonçalves. A prova digital no direito processual brasileiro. **Revista da Escola Superior do MPCE**, ano 13, n. 1, p. 11-34, jan./jul. 2021. Disponível em: https://revistaacademica.mpce.mp.br/revista/article/view/147/137. Acesso em: 01 maio 2023.

LERS. **Sistema de solicitação de aplicação da lei**. Disponível em: https://lers.google.com/signup_v2/landing. Acesso em: 10 out. 2023.

LERS-FAQ. **Esclarecimentos sobre dados e informações produzidas pela Google LLC**. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/fff5c989-1035-4435-9697-13c52c43a612. Acesso em: 10 out. 2023.

LOPES, O. A. **Fundamentos da regulação**. Rio de Janeiro: Processo, 2018.

MACHADO, Fernanda Pereira da Silva. **A nulidade das provas digitais**. **Consultor Jurídico**, 05 de outubro de 2022. Disponível em: https://www.conjur.com.br/2022-out-05/fernanda-machado-nulidade-provas-digitais. Acesso em: 5 maio 2023.

Magno, L. E; COMPLOIER, M. Cadeia de custódia da prova penal. **Cadernos Jurídicos**, São Paulo, v. 22, n. 57, p. 195-219, jan./mar. 2021. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/150396. Acesso em: 10 jul. 2023.

MAIA, Francisco Silvio. **Criminalística geral**. 2012. Disponível em: http://tmp.mpce.mp.br/esmp/apresentacoes/I_Curso_de_Investigacao_Criminal_Homic%C3%ADdio/02_Criminalistica_Geral_29_11_2012.pdf. Acesso em: 29 set. 2023.

MALTA, Alberto *et al*. De Daubert a Schauer: reflexões sobre admissibilidade e valoração das provas científicas. COSTA-NETO, João; AMATO, Lucas Fucci; BUSTAMANTE, Thomas (org.) **A prova**: ensaio em homenagem a Frederick Schauer. Rio de Janeiro: Lumen Juris, 2023. v. III. p. 189-227. (Coleção Fundamentos do Direito).

MARTINI, Lucas Cardoso. **O standard Daubert e sua possível aplicação no contexto jurídico brasileiro**. 2015. Monografia (Graduação) – Faculdade de Direito, Universidade Federal do Rio Grande de Sul, Porto Alegre, 2015. Disponível em: https://lume.ufrgs.br/handle/10183/183701. Acesso em: 12 out 2023.

MASSENA, C. B. A propósito da cadeia de custódia das provas digitais no processo penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa. **Boletim IBCCRIM,** ano 31, n. 368, p. 19-21, jul. 2023.

MENDES, Lucas. STF dá 24 horas para que Telegram indique representante legal no Brasil. **CNN Brasil**, 23 de maio de 2023. Disponível em: https://www.cnnbrasil.com.br/politica/moraes-determina-que-telegram-indique-representantes-legais-no-brasil-em-24h-sob-pena-de-suspensao-do-app/. Acesso em: 20 ago. 2023.

MINTO, A O. **A prova digital no processo penal**. São Paulo: LiberArts, 2021.

MJ. Ministério da Justiça - Secretaria de Segurança Pública. **Portaria n. 82 de 16 de julho de 2014**. Estabelece as Diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígios. Disponível em: https://diariofiscal.com.br/ZpNbw3dk20XgIKXVGacL5NS8haIoH5PqbJKZaawfaDwCm/legislacaofederal/portaria/2014/senasp82.htm. Acesso em: 6 maio 2023.

MJ. Ministério da Justiça - Secretaria de Segurança Pública. **Procedimento operacional padrão:** perícia criminal. 2013. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf. Acesso em: 01 maio 2023.

MJ. Ministério da Justiça e Segurança Pública. **Cooperação Internacional em Matéria Penal**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal. Acesso em: 30 abr. 2023.

MJ. Ministério da Justiça e Segurança. **Cooperação Internacional em matéria penal**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal. Acesso em: 03 maio 2023.

MJ. Ministério da Justiça e Segurança. **Perguntas frequentes - Acordos Internacionais em matéria penal**. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/perguntas-frequentes/ativos_cooperacao/materia-penal-1. Acesso em: 30 abr. 2023.

MP/PR. Ministério Público do Paraná. Oficinas para o desenvolvimento de protocolos de investigação. **Cadeia de Custódia – Portaria 82-014/SENASP**. Disponível em:

https://criminal.mppr.mp.br/arquivos/File/Cadeia_de_Custodia_PORTARIA_SENASP_N_82DE_16_DE_JULHO. Acesso em: 02 maio 2023.

NERES, W F. A cadeia de custódia dos vestígios digitais sob a ótica da Lei n. 13.964/2019: aspectos teóricos e práticos. **Boletim Científico – ESMPU**, ano 20, n. 56, p. 338-382, jan./jun. 2021. Disponível em: https://escola.mpu.mp.br/publicacoes/boletim-cientifico/edicoes-do-boletim/boletim-cientifico-n-56-janeiro-junho-2021/a-cadeia-de-custodia-dos-vestigios-digitais-sob-a-otica-da-lei-n-13-964-2019-aspectos-teoricos-e-praticos. Acesso em: 21 set. 2023.

NIGRI, Deborah Fisch. **Crimes e segurança na internet**. Caxias do Sul: Plenum, 2001.

NIST. National Institute of Standard and Technology. Guidelines for media sanitization. NIST **SP 800-88**. Rev. 1, 2014. Disponível em: https://csrc.nist.gov/pubs/sp/800/88/r1/final. Acesso em: 18 jul 2023.

NIST. National Institute of Standards and Technology. The NIST definition of cloud computing: recommendations of the National Institute of Standards and Technology. **Special Publication 800-145**. 2011. Disponível em: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Acesso em: 04 fev. 2017.

OLIVEIRA, **Robson Rocha de.** Dos conceitos de regulação às suas possibilidades. **Saúde e Sociedade**, São Paulo, v. 23, n. 4, p. 1198-1208, 2014. Disponível em: https://www.scielo.br/j/sausoc/a/pkTKqybVJWpgbR6D4VfdwHt/?format=pdf&lang=pt. Acesso em: 20 ago. 2023.

OLIVEIRA, Vinícius Machado. **Evidência digital**. 2023. Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/. Acesso em: 20 jun. 2023.

PARODI, Lorenzo. A cadeia de custódia da prova digital à luz da Lei 13.964/2019 (Lei anticrime). **Migalhas**, n. 5.717, de 30 de outubro de 2023. Disponível em: https://migalhas.uol.com.br/depeso/320583/a-cadeia-de-custodia-da-prova-digital-a-luz-da-lei-13-964-19--lei-anticrime. Acesso em: 24 fev. 2021.

PASTORE, Alexandro Mariano; FONSECA, Manoel Augusto Cardoso. Cadeia de custódia de provas digitais nos processos do direito administrativo sancionador com a adoção da tecnologia Blockchain**. Cadernos tecnológicos da CGU**, v. 3, p. 97-109, 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/597. Acesso em: 20 ago. 2023.

PEDROSA, Paulo H.C.; NOGUEIRA, Tiago. Computação em nuvem. *In*: V Seminário de Tecnologia, Gestão e Educação, maio de 2011. **Anais** [...]. Disponível em: https://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04- 09 5352-120531-t2.pdf. Acesso em: 20 ago. 2023.

PEREIRA, A. M. G. Autogoverno, regulação, função normativa e independência interna no judiciário. **Revista de Direito Setorial e Regulatório**, Brasília, v. 2, n. 2, p. 1-46, outubro 2016. Disponível em: https://periodicos.unb.br/index.php/rdsr/article/view/19223/17726. Acesso em: 10 out. 2023.

PEREIRA FILHO, Benedito Cerezzo *et al*. Fake News e Hate Speech: La Genesi dei Linciagci?. **Manual de Direito na Era Digital: Penal e Internacional**. PINHO, A C, et al. Indaiatuba,SP: Editora Foco, 2023. (Coletânea de Manuais de Direito Digital).

PINHEIRO, Patricia Peck. **Direito digital**. 5. ed. São Paulo: Saraiva, 2013.

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva, 2021.

PINHEIRO, Patricia Peck. Sobre a adesão do Brasil à Convenção de Budapeste. **Tele.Síntese**, 14 abril de 2023. Disponível em: https://www.telesintese.com.br/peck-sobre-a-adesao-do-brasil-a-convencao-de-budapeste/. Acesso em: 02 set. 2023.

PLACHA, Gabriel. **A Atividade regulatória do estado**. 2007. 257 f. Dissertação (Mestrado em Direito) – Setor de Ciências Jurídicas e Sociais, Direito, Pontifícia Universidade Católica do Paraná, Curitiba, 2007.

PRADO, G. **A cadeia de custódia da prova no processo penal**. 2. ed. São Paulo: Marcial Pons, 2021.

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

PROJETO E-EVIDENCE. Disponível em: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en. Acesso em: 01 maio 2023.

PUGLIESE, Y S; LUIZ, J H B. Os desafios da adesão à Convenção de Budapeste sobre o crime cibernético. **Consultor Jurídico**, 10 de janeiro de 2022. Disponível em: https://www.conjur.com.br/2022-jan-10/opiniao-desafios-brasil-adesao-convencao-budapeste. Acesso em: 02 maio 2023.

RAFFUL, Leonardo José; RAFFUL, Ana Cristina. Prova eletrônica. **Revista do Direito Público**, Londrina, v. 12, n. 2, p. 48-76, ago. 2017. Disponível em: http:// www.uel.br/revistas/uel/index. php/direitopub/article/view/26212. Acesso em: 14 set. 2023.

RAMOS, Paulo Henrique; FARIAS JUNIOR, Ivaldir H. **Os desafios da computação em nuvem como serviço**. 2020. Dissertação (Mestrado) – Faculdade Joaquim Nabuco, Recife, 2020. Disponível em: https://arquivei.com.br/blog/armaze namento-em-nuvem-o-que-e/. Acesso em: 27 ago. 2023.

RAND CORPORATION. **Interactive tool for ranking digital evidence needs**. Disponível em: https://www.rand.org/well-being/justice-policy/projects/priority-criminal-justice-needs/digital-evidence-needs/interactive-tool.html. Acesso em: 12 out. 2023.

ROCKEMBACH, Moisés. Evidência da Informação em plataformas digitais: da reflexão teórica à construção de um modelo. **Informação Arquivística**, v. 2, n. 1, p. 89-109, 2013. Disponível em: https://www.brapci.inf.br/_repositorio/2015/12/pdf_a9c97a9 a 67_0000018247.pdf. Acesso em: 16 ago. 2023.

RODRIGO, Fernando M. La evidencia digital en el proceso penal y la preservación de los derechos fundamentales. **Revista Escola Superior do Ministério Público do Ceará**, ano 13, n. 211, p. 135-161, 2021. Disponível em: www.revistaacademica.mpce.mp.br. Acesso em: 28 ago. 2023.

RODRIGUES, Benjamim Silva. **Direito penal:** parte especial.. Coimbra: Coimbra, 2009. t. I. (Direito Penal Informático-Digital)

ROSA, A M; VIEIRA, M R. Cloud Act: quando a investigação se dá nas nuvens americanas. **Consultor Jurídico**, 22 de novembro de 2019. Disponível em: https://www.conjur.com.br/2019-nov-22/limite-penal-cloud-act-quando-investigacao-nuvens-americanas. Acesso em: 01 maio 2023.

ROSA, Alexandre Morais da. A prática de fishing expedition no processo penal. **Consultor Jurídico**, 02 de julho de 2021. Disponível em: https://www.conjur.com.br/2021-jul-02/limite-penal-pratica-fishing-expedition-processo-penal. Acesso em: 08 jun. 2023.

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

RUAN, Keyun *et al*. Cloud forensics. *In*: PETERSON, Gilbert; SHENOI, Sujeet. Advances in digital forensics VII: 7th IFIP WG 11.9 **International Conference on Digital Forensics**. Orlando: Springer, 2011. cap. 2. p. 1-12. Disponível em: http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf. Acesso em: 02 maio 2023.

SANT'ANA, Jéssica. Aneel aprova política de segurança cibernética a ser adotada pelos agentes do setor. **Portal G1**, 14 de dezembro de 2021. Disponível em: Disponível em: https://g1.globo.com/economia/noticia/2021/12/14/aneel-aprova-politica-de-seguran ca-cibernetica-a-ser-adotada-pelos-agentes-do-setor.ghtml. Acesso em: 06 maio 2023.

SANT'ANA, Jéssica. Aneel aprova política de segurança cibernética a ser adotada pelos agentes do setor, **Portal G1**, de 14 de dezembro de 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/12/14/aneel-aprova-politica-de-seguranca-cibernetica-a-ser-adotada-pelos-agentes-do-setor.ghtml. Acesso em: 06 maio 2023.

SCHAUER, Frederick. **The proof**: uses of evidence in law, politics and everything else. Cambridge: Harvard University Press, 2022.

SILVA NETO, Sertório de Amorim e. O que é um paradigma?. **Revista de Ciências Humanas,** v. 45, n. 2, p. 345-354, 2011. Disponível em: https://periodicos.ufsc.br/index.php/revistacfh/article/view/2178-4582.2011v45n2p345/22356. Acesso em: 28 ago. 2023.

SOUZA *et al*. **Manual prático de provas digitais**. São Paulo: Thompson Reuters Brasil, 2023.

SOUZA, Déborah da Paz. **Proteção de dados e o processo penal**: desafios e parâmetros da cadeia de custódia da prova digital. 2021. 64 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2021. Disponível em: https://bdm.unb.br/handle/10483/28900. Acesso em 19 out. 2023.

SVANTESSON, D. **The EU's approach to e-Evidence**. Disponível em: https:// directionsblog.eu/the-eus-approach-to-e-evidence/. Acesso em: 31 mar. 2022.

SWIRE, P; DASKAL, J. Frequently asked questions about the U.S. Cloud Act. **The Cross-Border Data Forum (CBDF**), april 16, 2019. Disponível em: https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/. Acesso em: 30 abr. 2022.

TAURION, Cezar. **Cloud computing**: transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2008.

TAVARES NETO, José Querino; KOZICKI, Katya. DO "EU" PARA O "OUTRO": A ALTERIDADE COMO PRESSUPOSTO PARA UMA (RE) SIGNIFICAÇÃO DOS DIREITOS HUMANOS. **Revista da Faculdade de Direito UFPR**, Curitiba, jun. 2008. ISSN 2236-7284. Disponível em: <https://revistas.ufpr.br/direito/article/view/15735>. Acesso em: 06 nov. 2023. doi:http://dx.doi.org/10.5380/rfdufpr.v47i0.15735.

THAMAY, Rennan; TAMER, Maurício. **Provas no direito digital**: conceito da prova digital: procedimentos e provas digitais em espécie. São Paulo: Revista dos Tribunais, 2020. Disponível em: https://www.jusbrasil.com.br/doutrina/provas-no-direito-digital-conceito-da-prova-digital-procedimentos-e-provas-digitais-em-especie/1147564455. Acesso em: 02 maio 2023.

THAMAY, Rennan; TAMER, Maurício. **Provas no direito digital**: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. [Livro Eletrônico].

TIBCO. **O que é computação em nuvem distribuída?**. Disponível em: https://www.tibco.com/pt-br/reference-center/what-is-distributed-cloud-computing. Acesso em: 12 jun. 2023.

UE. Comissão Europeia. **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às Ordens europeias de entrega ou de conservação de provas eletrônicas em matéria penal**. 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0225&from=PT. Acesso em: 01 maio 2023.

UE. Council of the European Union. **Proposal for a regulation of the European parliament and of the council, on European Production and preservation orders for electronic evidence in criminal matters**. 2019. Disponível em: https://www.crossborderdataforum.org/wp-content/uploads/2019/10/EU-Council-E-Evidence-Draft-06.11.19.pdf. Acesso em: 31 mar. 2023.

UE. European Union. **The Council adopts its negotiating mandate for a new EU**

law on liability for defective products. 14 junho 2023. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/. Acesso em: 21 ago. 2023.

VASCONCELOS, Fernando Antônio de. **Internet**: responsabilidade do provedor pelos danos praticados. Curitiba: Juruá, 2003.

VASYUKOV, V.; ILDUZOVNA KHISAMOVA, Z. Investigation and Seizure of Electronic Media in the Production of Investigative Actions. **Law, State and Telecommunications Review**, v. 13, n. 2, p. 78-88, 2021. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/25920. Acesso em: 17 out. 2023.

VAZ, Denise Provasi. **Provas digitais no processo penal**: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese. (Doutorado em Direito Processual) – Universidade de São Paulo. São Paulo. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/publico/Denise_Provasi_Vaz_tese_integral.pdf. Acesso em: 16 ago. 2023.

VAZQUEZ MAYMIR, S. Anchoring the need to revise cross-border access to e-evidence. **Internet Policy Review**, v. 9, n.3, 2020. Disponível em: https://policyreview.info/articles/analysis/anchoring-need-revise-cross-border-access-e-evidence. Acesso em: 31 mar. 2022.

VERIFACT. **Solução online mais confiável para o registro de provas digitais na Internet**. Disponível em: https://www.verifact.com.br/?utm_source=google&utm_medium=cpc&utm_campaign=google-pesquisa-verifact-verifact&gclid=Cj0KCQjw6KunBh DxARIsAKFUGs8qPwqZ7-GjFX_Bg3twJl40XX2. Acesso em: 23 ago. 2023.

VERMEER, Michael J. D.; DULANI Woods; BRIAN A. Jackson. **Identifying law enforcement needs for access to digital evidence in remote data centers**. Santa Monica, CA: RAND Corporation, 2018. Disponível em: https://www.rand.org/pubs/research_reports/RR2240.html. Acesso em: 01 out. 2023.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. Dissertação (Mestrado) – Faculdade de Direito, Universidade de Brasília, Brasília, 2007.

VILAR, Gustavo P; GUSMÃO, Luiz E. Identificação, isolamento, coleta e preservação do vestígio cibernético. *In*: VELHO, Jesus Antônio. (org.) **Tratado de computação forense**. São Paulo: Millennium, 2016. cap. 1.

WAHL, T. **Comission proposes legislative framework for e-evidence**. Disponível em: https://eucrim.eu/news/commission-proposes-legislative-framework-e-evidence/. Acesso em: 31 mar. 2023.

WERTHEIN, Jorge. A sociedade da informação e seus desafios **CI. Inf**., v. 29, n. 2, p. 71-77, 2000. Disponível em: www.scielo.br. Acesso em: 28 ago. 2023.

ZAMIDI, Ettore. **A questão do documento eletrônico no Código de Processo Civil de 2015**. Disponível em: https://www.conjur.com.br/2019-jan-06/ettore-zamidi-

questao-documento-eletronico-cpc2015. Acesso em: 13 set. 2023.