

## **Blockchain e processo penal: os reflexos dos avanços tecnológicos na confiabilidade da prova penal**

### **Blockchain and criminal proceedings: the effects of technological advances on the reliability of criminal evidence**

Matheus Dantas Vilela\*  
Daniel Araújo de Assis\*\*  
Pablo Eduardo\*\*\*

#### **RESUMO**

O progresso tecnológico trouxe uma série de desafios complexos para o sistema de justiça, especialmente no contexto do processo penal, onde a confiabilidade das provas digitais desempenha um papel crucial. A disseminação cada vez maior de evidências digitais, como conversas no *WhatsApp*, suscita preocupações significativas sobre sua integridade e autenticidade devido à possibilidade sempre presente de adulteração. Nesse cenário, a tecnologia *blockchain* emerge como uma solução promissora para garantir a confiabilidade dessas provas. A *blockchain*, originalmente concebida para assegurar a segurança das transações de criptomoedas, oferece uma abordagem eficaz para preservar a integridade das evidências digitais. Ao registrar transações de forma imutável e transparente em uma rede descentralizada, a *blockchain* garante a autenticidade e a integridade das provas desde o momento da coleta até sua apresentação em juízo. Além disso, a tecnologia *blockchain* pode ser explorada na investigação defensiva, permitindo que a defesa colete e preserve provas de maneira independente. Este artigo propõe investigar os impactos da tecnologia *blockchain* na confiabilidade das provas digitais no contexto do processo penal. Por meio de uma abordagem interdisciplinar que combina conhecimentos jurídicos e tecnológicos, o estudo busca explorar o potencial da *blockchain* como uma ferramenta para garantir a integridade e a autenticidade das evidências digitais no processo penal. Ao promover essa análise, o artigo visa contribuir para o avanço do debate sobre a aplicação da tecnologia *blockchain* no sistema de justiça, oferecendo insights e recomendações para aprimorar os métodos de coleta e apresentação de provas no processo penal, garantindo sua eficácia diante dos desafios impostos pela era digital.

**Palavras-chave:** prova digital; blockchain; cadeia de custódia; investigação defensiva.

#### **ABSTRACT**

---

Artigo submetido em 2 de maio de 2024 e aprovado em 28 de maio de 2025.

\* Mestrando pelo Programa de Pós-graduação em Direito da PUC/MG, na linha de pesquisa "Intervenção Penal e Garantismo" - Bolsista CAPES/PROEX. Membro do grupo de pesquisa "Direito Penal Contemporâneo: em busca da maior proteção com o menor sacrifício à liberdade" (PUC/MG - CNPq). Especialista (pós-graduação lato sensu) em Direitos Humanos pelo Curso CEI e em Advocacia Criminal pela Escola Superior de Advocacia da OAB/MG. Bacharel em Direito pela PUC/MG. Advogado Criminalista. E-mail: [mdvilelaji@gmail.com](mailto:mdvilelaji@gmail.com)

\*\* Especialista (pós-graduação lato sensu) em Direito Público pela Pontifícia Universidade Católica do Rio Grande do Sul e em Advocacia Cível pela Escola Superior de Advocacia do Conselho Federal da OAB. MBA em Gestão e Inovação pela Escola Superior de Advocacia da OAB/MG. Bacharel em Direito pela PUC/MG. Advogado. E-mail: [daniel.araujo.assis@gmail.com](mailto:daniel.araujo.assis@gmail.com)

\*\*\* Aluno de disciplina isolada no Programa de Pós-graduação em Direito da PUC/MG. Especialista (pós-graduação lato sensu) em Processo Penal pelo Curso CEI e em Advocacia Cível pela Escola Superior de Advocacia da OAB/MG. Bacharel em Direito pela PUC/MG. Advogado criminalista. E-mail: [paeduardoadv@gmail.com](mailto:paeduardoadv@gmail.com)

Technological progress has brought a series of complex challenges to the legal system, especially in the context of criminal proceedings, where the reliability of digital evidence plays a crucial role. Each time greater digital evidence occurs, such as conversations on WhatsApp, it raises concerns about its integrity and occurrences due to the ever-present possibility of tampering. In this scenario, blockchain technology emerges as a promising solution to guarantee the reliability of these proofs. Blockchain, originally designed to ensure the security of cryptocurrency transactions, offers an effective approach to preserving the integrity of digital evidence. By recording transactions in an immutable and transparent way on a decentralized network, blockchain guarantees the protection and integrity of evidence from the moment it is collected until it is presented in court. Furthermore, blockchain technology can be exploited in defensive investigation, allowing the defense to independently collect and preserve evidence. This article proposes to investigate the impacts of blockchain technology on the reliability of digital evidence in the context of criminal proceedings. Through an interdisciplinary approach that combines legal and technological knowledge, the study seeks to explore the potential of blockchain as a tool to guarantee the integrity and protection of digital evidence in criminal proceedings. By promoting this analysis, the article aims to contribute to the advancement of the debate on the application of blockchain technology in the judicial system, offering insights and recommendations to improve methods of collecting and presenting evidence in criminal proceedings, ensuring their effectiveness in the face of challenges imposed by the digital age.

**Keywords:** digital evidence; blockchain; chain of custody; defensive investigation.

## 1 INTRODUÇÃO

Na contemporaneidade, a rápida evolução tecnológica alterou profundamente a maneira como armazenamos e compartilhamos informações. A pandemia da COVID-19 acelerou ainda mais essa mudança, levando à integração generalizada de ferramentas digitais em nosso cotidiano para lidar com os desafios impostos pela crise sanitária.

Mesmo após o término da pandemia, o progresso tecnológico continua avançando, trazendo consigo desafios complexos, como o aumento dos crimes cibernéticos e a sofisticação das técnicas de manipulação digital, a exemplo da criação de vídeos *deepfake* e a edição de mensagens em aplicativos de comunicação, como o *WhatsApp*. Esses avanços têm gerado uma crescente preocupação com a confiabilidade das provas digitais no contexto do processo penal.

A disseminação de provas digitais no processo penal, como capturas de tela de (*print screen*), traz consigo a possibilidade de adulteração e manipulação, comprometendo a integridade e autenticidade das evidências apresentadas em juízo. Diante desse cenário, surge a necessidade de atualizar os métodos de coleta probatória para garantir sua confiabilidade perante o sistema judicial.

Por outro lado, o desenvolvimento da tecnologia *blockchain* oferece uma solução promissora para os desafios relacionados à confiabilidade das provas digitais. Inicialmente concebida para garantir a segurança e transparência das transações de criptomoedas, a *blockchain* apresenta-se como uma ferramenta eficaz para preservar a integridade das evidências digitais no processo penal.

Ao registrar de forma imutável e transparente as transações digitais em uma cadeia de blocos interconectados, a *blockchain* garante a autenticidade e integridade das provas desde sua coleta até sua apresentação em juízo. Essa tecnologia oferece uma camada adicional de segurança, dificultando a adulteração ou falsificação das evidências, e promovendo a confiança no sistema de justiça.

Além disso, a tecnologia *blockchain* também emerge como uma ferramenta promissora

na investigação defensiva, oferecendo à defesa a capacidade de coletar e preservar provas digitais de forma independente. Dessa forma, a *blockchain* pode contribuir para equilibrar a relação entre acusação e defesa.

Diante desse contexto, este trabalho tem como objetivo investigar os impactos da tecnologia *blockchain* na confiabilidade das provas digitais no processo penal. Por meio de uma abordagem interdisciplinar que combina conhecimentos das ciências penais e da tecnologia, busca-se explorar o potencial da *blockchain* como uma ferramenta para garantir a integridade e autenticidade das evidências digitais no contexto judicial.

Ao promover essa análise, espera-se contribuir para o avanço do debate sobre a aplicação da tecnologia *blockchain* no sistema judicial, oferecendo insights e recomendações para aprimorar os métodos de coleta e apresentação de provas no processo penal, e garantir decisões justas do sistema judicial frente aos desafios impostos pela era digital.

## 2 O PAPEL DA JUSTIÇA NO ADVENTO DAS NOVAS TECNOLOGIAS

A era da informação pode ser definida como o núcleo central de nossa contemporaneidade. O paradigma de vida proposto no período pós-revolucionário difere substancialmente do anterior. Observa-se uma transição da homogeneização e uniformidade para a personalização e diversificação de produtos e serviços. Mesmo para os protagonistas desta nova era, abordar retrospectivamente o passado apresenta-se como uma empresa desafiadora; as conjecturas sobre o que hoje vivenciamos remontam ao último século.<sup>1</sup>

As fundações dessa era remontam a períodos ainda mais remotos, datando desde Johannes Gutenberg, que adaptou a invenção chinesa da tipografia para o Ocidente no século XV. Avançamos através das contribuições de figuras proeminentes como Charles Babbage, com sua Máquina Analítica, Alexander Graham Bell, inventor do telefone, Konrad Zuse, que introduziu o conceito de dígito binário ou simplesmente *bit*, e ainda Bill Gates, fundador da Microsoft, bem como Steven Jobs e Stephen Wozniak, os criadores da Apple. Todas essas personalidades foram cruciais na emergência de uma era que agora nos é tão familiar e imersiva que nossa imaginação constantemente especula sobre o que o futuro nos reserva.

A imposição do isolamento social em resposta à pandemia da COVID-19 não passou despercebida, tendo implicado não apenas uma atenção ampliada à saúde coletiva e individual, mas também validado previsões relacionadas ao ensino à distância (EAD) e ao trabalho remoto. Atualmente, o foco do debate reside na especulação sobre o comportamento da sociedade em um cenário pós-pandemia. “A tecnologia veio para ficar” tem se tornado o mantra predominante da humanidade.

O contato social, que desempenha um papel crucial na natureza gregária do ser humano, está gradativamente migrando para o domínio virtual. Plataformas de redes sociais como *Facebook*, *Twitter* e *WhatsApp* proporcionam interações humanas que atendem às expectativas de maneira satisfatória. Neste contexto, surge um debate relevante acerca da preservação de direitos e garantias fundamentais, especialmente em um período caracterizado pelo aumento exponencial da incidência de crimes virtuais.<sup>2</sup>

---

<sup>1</sup> A título de ilustração, uma matéria da Revista Superinteressante publicada em 1994 já previa o amplo acesso aos smartphones e o trabalho remoto, assim como diversas outras transformações já incorporadas à sociedade mundial contemporânea. (Barreira, 1994)

<sup>2</sup> Segundo dados da Central Nacional de Denúncias de Crimes Cibernéticos – uma parceria, da ONG Safernet Brasil com o Ministério Público Federal (MPF) –, o número de denúncias anônimas de crimes cometidos pela internet mais que dobrou em 2020. De janeiro a dezembro do ano passado, foram 156.692 denúncias anônimas, contra 75.428 em 2019 (Globo, 2021a).

Na operacionalização da Justiça, essa mudança desencadeou uma revolução de magnitude considerável.<sup>3-4</sup> No Brasil, a adoção da tramitação eletrônica de processos físicos possibilita que advogados de diversas localidades representem clientes separados por longas distâncias geográficas. A digitalização integral do conjunto de evidências probatórias e a realização de audiências por meio de videoconferência são exemplos de facilidades que têm o potencial de aumentar a acessibilidade ao sistema judiciário.<sup>5</sup>

Alguns argumentam que a convivência da tecnologia em nosso espaço é uma realidade há muito tempo. No entanto, o Poder Judiciário parece demonstrar certa lentidão na adaptação e inovação, mantendo condutas e práticas dispensáveis. Essas práticas, muitas vezes, são justificadas em nome de uma suposta segurança jurídica, mas, na verdade, refletem um conservadorismo repreensível. A mudança comportamental observada no *homo sapiens* tem impacto direto no campo do Direito, tornando impossível conceber a atividade jurídica – eminentemente intelectual – sem o suporte de máquinas, *softwares* e inteligência artificial na gestão processual. Assim, reconciliar-se com o progresso torna-se um pressuposto essencial para garantir uma prestação jurisdicional satisfatória.

É inegável que os desafios enfrentados pelo sistema judiciário estão intrinsecamente relacionados à insegurança trazida pelas novas tecnologias. Embora a conexão entre o mundo virtual e a evolução civilizatória tenha promovido inclusão, imediação e acesso à informação, também observamos o surgimento de comportamentos prejudiciais e o aumento dos riscos já existentes. Além dos benefícios amplamente anunciados, enfrentamos questões como o compartilhamento não autorizado de dados pessoais, ofensas à intimidade e à honra, danos ao patrimônio, adulterações de documentos e páginas da *web*, bem como a proliferação de perfis falsos em toda a rede, juntamente com inúmeras invasões perpetradas por *hackers* (Simantob, 2012, p. 61-62).

### 3 CRIMES CIBERNÉTICOS E PROVA DIGITAL NO PROCESSO PENAL

Os crimes cibernéticos são uma realidade na sociedade contemporânea e, com a crescente implementação do uso da internet pelos mais variados segmentos e diferentes finalidades, vieram à tona os movimentos político-criminais com demandas por criminalização e repressão ainda no final na década de 1990. A Convenção sobre o Crime Cibernético, também conhecida como Convenção de Budapeste, tratado aberto em 23/11/2001 para adesão de Estados-membros e não-membros do Conselho da Europa<sup>6</sup>, é o primeiro e único instrumento internacional vinculativo sobre a questão, servindo como diretriz para outros países que estejam desenvolvendo uma legislação nacional abrangente contra o crime cibernético e como uma estrutura para a cooperação internacional entre Estados. (Cidrão; alves; muniz, 2018, p. 77-79)

Basicamente, os crimes cibernéticos podem ser classificados em: (i) crimes cibernéticos puros, que tutelam bens jurídicos de natureza informática; (ii) crimes cibernéticos mistos, que

---

<sup>3</sup> Segundo Dierle Nunes (2020, p. 15), é a chamada “virada tecnológica”. A expressão decorre de um paralelo com outras revoluções, a saber: (i) virada constitucional, indicando os impactos da constitucionalização do Direito, sobretudo no segundo pós-guerra; (ii) virada cognitiva, decorrente da percepção dos impactos das heurísticas e vieses cognitivos no Direito; (iii) virada linguística-ontológica, significando o abandono da linguagem como instrumento de comunicação, reconhecendo-a como condição de possibilidade.

<sup>4</sup> Já se fala na instituição de Cortes de Justiça completamente virtuais, sem qualquer instalação física. O jurista americano Richard Susskind (2019) teoriza sobre a questão em seu livro, “Online Courts and the Future of Justice”, que ganhou certa notoriedade em virtude da pandemia da COVID-19.

<sup>5</sup> No final de 2020, o Conselho Nacional de Justiça aprovou a Resolução nº 345, em que autoriza e regulamenta a prática do “Juízo 100º Digital”, permitindo que os atos processuais de uma demanda sejam completamente praticados pela via eletrônica, tornando desnecessário o comparecimento físico aos fóruns e tribunais. (BRASIL, 2020a)

<sup>6</sup> Apesar da Convenção sobre o Crime Cibernético ter sido firmada pela República Federativa do Brasil desde sua abertura, a promulgação do decreto de adesão ocorreu somente em 12/04/2023. (BRASIL, 2023)

não tutelam bens jurídicos de natureza informática, mas o emprego da internet é condição necessária para a execução do delito; e (iii) crimes cibernéticos comuns, que também não tutelam bens jurídicos de natureza informática e que a internet é um mero instrumento para a execução do delito, enquadrando-se nesta hipótese os crimes clássicos que não possuem forma vinculada (Pinheiro, 2001, p. 18).

Com a criação de tipos penais e a adaptação de delitos já existentes aos novos meios disponíveis, surgem desafios probatórios que vão além da simples identificação da autoria ou da demonstração da materialidade. Garantir a confiabilidade das evidências colhidas torna-se uma tarefa crucial no contexto jurídico contemporâneo. Mas se o avanço tecnológico e propagação da internet ocasionou novos processos de criminalização, também é verdade que tais mecanismos podem ser de grande valia até mesmo para a persecução criminal de delitos sem conteúdo cibernético<sup>7</sup> ou para uma defesa efetiva de acusados e evitar o gravíssimo erro judiciário que é a condenação de inocentes<sup>8</sup>.

A prova penal possui uma função cognitiva, consubstanciada na tentativa de uma reconstrução aproximada de fatos passados, sendo o acerto do juízo fático um dos requisitos para uma decisão justa. Ainda que a verdade no processo penal seja inalcançável e a metodologia de construção do conhecimento judicial conforme o modelo constitucional estabeleça limites e parâmetros, as provas produzidas com emprego de técnicas digitais podem trazer inestimáveis contribuições para a resolução de casos penais. (Badaró, 2019, p. 121)

Não pode ser desconsiderado que a persecução criminal se submete ao *due process of law*, condicionando a validade da prova penal ao acatamento da forma legal. Dentro dessa lógica inclui-se, como regra, a taxatividade dos meios de obtenção de prova no processo penal, restando somente autorizada o manejo das ferramentas dispostas em lei. Excepcionalmente, poderá ser admitido meios de obtenção de prova atípicos, mas desde que a produção desses elementos opere com técnica idônea, ainda mais em razão da obsolescência da legislação processual penal doméstica diante da evolução tecnológica, sendo vedada, contudo, a subversão da forma legal prevista para um meio de obtenção específico e práticas incompatíveis com os direitos fundamentais<sup>9</sup>. (Lopes Jr., 2020, p. 614)

Por isso, quando se mostra factível a produção probatória com emprego de técnica digital, é dever do polo acusatório a exploração de tais elementos, sob pena de absolvição do acusado pela perda de uma chance probatória<sup>10</sup>. Em contrapartida, a inércia do defensor técnico do acusado, a depender do contexto, pode ensejar no reconhecimento de uma defesa técnica deficiente pelo não desenvolvimento de uma atividade probatória mínima<sup>11</sup>.

<sup>7</sup> Como exemplo destacamos o programa “Olho Vivo” da Polícia Militar de Minas Gerais, cujo sistema de monitoramento conseguiu impedir a consumação de um delito de estupro no município de Juiz de Fora (MG). (Globo, 2021b)

<sup>8</sup> Para fins de ilustração cita-se a linha do tempo do *Google Maps* para comprovação de álbis, funcionalidade disponibilizada em *smartphones android* que registra os locais e trajetos do usuário com os respectivos horários. (Google, 20--)

<sup>9</sup> Prática dissuadida no sistema de justiça criminal brasileiro é o reconhecimento pessoal em detrimento da forma prevista no art. 226 do Código de Processo Penal. Após vários anos, o Superior Tribunal de Justiça, em decisão histórica sobre o tema e representativo da virada jurisprudencial, não passou mais a admitir o reconhecimento pessoal que não segue a forma legal (Brasil, HC nº 598.886/SC, 2020b). Diante da relevância da matéria e visando evitar erros judiciais decorrentes da memória humana, o Conselho Nacional de Justiça editou a Resolução n. 484 para estabelecer diretrizes para o reconhecimento pessoal (Brasil, 2022).

<sup>10</sup> A condenação penal demanda a satisfação do *standard* de prova além da dúvida razoável, de modo que devem ser afastadas as hipóteses compatíveis com a inocência do acusado. Se a acusação se omite na produção de determinado elemento de prova factível com amplitude explicativa, especialmente diante de tantos meios tecnológicos disponíveis atualmente, incide a regra resolutive do *in dubio pro reo*. Nesse sentido, Rosa e Rudolfo (2017, p. 467) asseveram que a Teoria da Perda de uma Chance “pode ser invocada no processo penal para o fim de justificar teoricamente a absolvição pela falta de provas possíveis, não apuradas, não produzidas, mas factíveis, prevalecendo a presunção de inocência”.

<sup>11</sup> A jurisprudência da Corte Interamericana de Direitos Humanos é uníssona em afirmar que a designação de um defensor com o simples propósito de cumprir uma formalidade processual penal equivale a não ter defesa

Assim, apesar dos desafios que essa nova realidade apresenta, os avanços tecnológicos podem permitir um esclarecimento mais preciso das imputações criminais. Enquanto ao Estado-acusação incumbe o ônus de comprovar, de forma íntegra e coerente, a hipótese acusatória (Beltrán, 2017, P. 165), utilizando técnicas digitais idôneas; foi possibilitado ao defensor uma gama de oportunidades a serem aproveitadas, via investigação defensiva<sup>12</sup>, na demonstração de contra-hipóteses compatíveis com a inocência do acusado. Isso contribui para equilibrar minimamente a relação assimétrica entre as partes do processo penal quanto à capacidade de produção probatória, considerando que, embora a advocacia seja um múnus público, trata-se de uma atividade privada que não goza da fé pública inerente aos servidores públicos (Bulhões, 2019, p. 88-91).

Dessa forma, a implementação de técnicas de obtenção de provas digitais e a garantia de sua confiabilidade devem ser encaradas como responsabilidades de todos os sujeitos processuais, e é nesse contexto que se destaca o uso da tecnologia *blockchain*.

#### 4 A *BLOCKCHAIN* E A CONFIBILIDADE DAS PROVAS DIGITAIS NO PROCESSO PENAL

Com o surgimento das criptomoedas e a conseqüente necessidade de impedir qualquer interferência humana em tais operações, surgiu a criptografia via *blockchain*. Seu conceito surgiu quando Satoshi Nakamoto (pseudônimo do suposto criador do *bitcoin*) publicou o artigo acadêmico intitulado “Bitcoin: um sistema financeiro eletrônico peer-to-peer” (2008). Ali, a *blockchain* é definida como uma rede que marca o tempo das transações, colocando-as em uma cadeia contínua no *hash*, formando um registro que não pode ser alterado sem refazer todo o trabalho. Basicamente, tal tecnologia surgiu para que o *bitcoin* pudesse existir.

A *blockchain* é um sistema inovador de registro de informações, similar a um livro público e imutável. A tecnologia funciona através de uma rede descentralizada de computadores que armazena os dados em blocos interligados, como uma corrente. Cada bloco possui um *hash*, um código único que garante a integridade dos dados, o qual é calculado com base na informação antecedente. Se qualquer informação for alterada, o *hash* será recalculado, invalidando o código anteriormente gerado e comprometendo toda a corrente. Essa característica confere à tecnologia *blockchain* um considerável nível de segurança e confiabilidade. Além disso, o sistema é transparente, permitindo que qualquer pessoa possa verificar a autenticidade das transações<sup>13</sup>. (David; Minski, 2021, p. 8-10)

Evidentemente, a utilidade da *blockchain* não se esgota no mundo das criptomoedas, pois a confiabilidade da informação é necessária a todos setores da sociedade. Todavia, o presente trabalho possui um recorte específico de investigação: a *blockchain* como instrumento de

---

técnica, exigindo-se diligência nessa atividade. No *Caso Ruano Torres y otros vs. El Salvador*, a Corte IDH apontou o não desenvolvimento de uma atividade probatória mínima como o primeiro critério para aferição de uma defesa técnica deficiente. (Corte IDH, 2015, p. 49).

<sup>12</sup> O Provimento nº 188 de 2018 do Conselho Federal da OAB “regulamenta o exercício da prerrogativa profissional do advogado de realização de diligência investigatórias para instrução em procedimentos administrativos e judiciais”. (OAB, 2018)

<sup>13</sup> Em termos menos complexos: pense num trenzinho de brinquedo cujos trilhos estão espalhados pelo mundo inteiro. Não um, mas vários que formam uma rede global. Cada material vai dentro de um vagão, que é validado por máquinas espalhadas pelo mundo. Se aprovado, ele é selado com um código complexo de letras e números e se junta a outros vagões. Para aumentar ainda mais a segurança, cada vagão carrega seu código e o código do vagão anterior. Assim, caso alguém tente invadir um vagão, será preciso desvendar mais de um código. Essa rede de trenzinhos não tem dono, por isso todos os envios são registrados num livro disponível para qualquer um acessar. Mas não é possível ver o que foi enviado nem quem enviou, apenas quando houve o envio. Realizar todas essas operações é um pouco complexo. São poucas as pessoas que têm as máquinas necessárias para criar os códigos que selam os vagões e juntá-los com outros, por isso elas são remuneradas por esse trabalho (Leite, 2020).

garantia da confiabilidade da prova digital no processo penal.

A coerção penal é a expressão máxima da violência estatal contra o indivíduo, sendo sua legitimidade identificada pelo discurso jurídico nos esforços empreendidos em sua racionalização e limitação (Brandão, 2022, p. 31). Em razão disso, a coerção penal é condicionada a uma sentença penal condenatória que, por sua vez, é precedida por um procedimento persecutório que assegura garantias mínimas de proteção do imputado. O devido processo legal estabelece uma série de regras para apurar ações aparentemente delituosas, de modo que é fundamental a confiabilidade da prova penal para formação do juízo fático da imputação. (Ferrajoli, 2022, p. 73-107)

A prova no processo penal está estritamente ligada ao princípio da presunção de inocência, posto que a garantia, enquanto norma de controle da suficiência probatória, exige que as provas sejam suficientes para afastar todas as dúvidas razoáveis acerca da inocência do acusado. Caso contrário, não poderá haver sentença penal condenatória. Deste modo, a prova confiável é condição para o devido processo legal, pois legitima e limita a coerção penal. (Nardelii, 2018, p. 292-295)

Com o intuito de garantir a confiabilidade da prova penal, a Lei nº 13.964/19 (Pacote Anticrime) alterou o Código de Processo Penal para incluir o conceito e etapas da cadeia de custódia. Alexandre Morais da Rosa apresenta o seguinte conceito:

A Cadeia de Custódia é o instrumento de controle e garantia da integridade vestígios (dados de realidade) coletados durante a investigação preliminar e o processo penal. Os vestígios são os dados de realidade (mídias, instrumentos, sangue, digitais, DNA etc.) que analisados, passam a ser informação: evidência. A prova é o elemento, submetido ao contraditório, capaz de servir de mediador entre as Hipóteses (acusatória e/ou defensiva) e a decisão judicial. Situadas as distinções, em geral, toma-se um conceito pelo outro. Para fins de atribuição de culpa, a documentação do trajeto deve autorizar, de modo retrospectivo, o histórico cronológico da prova desde a obtenção do vestígio. O estabelecimento de regras, procedimentos e metodologias operacionais da Cadeia de Custódia tem o escopo de evitar a manipulação, o erro humano, a fraude, enfim, garantir as condições necessárias para que a evidência possa ser obtida, analisada, auditada e valorada, nas etapas subsequentes do processo penal. (Rosa, 2021, p. 400).

Portanto, é inegável o dever do Estado de preservar a prova, assegurando sua integridade, integralidade e confiabilidade. A cadeia de custódia garante que a prova colhida seja a mesma utilizada no processo. No entanto, quando se trata de provas digitais, os métodos tradicionais não são mais suficientes para garantir a confiabilidade da prova coletada. Isso se deve ao fato de não ser possível verificar se o arquivo digital coletado sofreu qualquer tipo de alteração. (Sombrio, 2021, p. 213)

A prova digital exige uma cadeia de custódia ainda mais detalhada, porque a linguagem digital é mais fácil de sofrer adulteração do que a linguagem natural da prova tradicional. Desse modo, a documentação da cadeia de custódia das provas digitais é fundamental para assegurar a confiabilidade da coleta, evitando qualquer tipo de dúvida quanto à existência de adulterações indevidas no material coletado. (Badaró, 2023, p. 181-183)

Para assegurar a confiabilidade da prova digital, é imprescindível garantir o controle e a transparência do material. Segundo Geraldo Prado, isso envolve uma análise cuidadosa de três características fundamentais dos dados digitais:

Relativamente aos dados digitais, a preservação da cadeia de custódia da prova é uma entre as diversas técnicas de certificação dos elementos apresentados, de modo que deverá responder aos questionamentos sobre a «integralidade» (o documento/objeto apresentado como prova se encontra da mesma forma em que foi originalmente adquirido?), a «espoliação» (houve alterações intencionais no documento/objeto durante o manuseio ou análise, ou a evidência em potencial foi destruída em antecipação a uma investigação?) e a «volatilidade» (o documento/objeto é suscetível de mudança

devido a fatores mecânicos, ambientais ou de passagem de tempo?). (Prado, 2021, p. 17)

O *print screen* de conversas do *WhatsApp* ilustra a facilidade de manipulação da prova digital. Existem aplicativos, como o *Fake WhatsApp Chat Generator*, que simulam facilmente uma conversa. Além disso, o *WhatsApp* permite editar e apagar mensagens, tirando o contexto original da conversa. Se não fosse suficiente, o aplicativo utiliza a tecnologia de encriptação de ponta a ponta, o que impede a recuperação de mensagens apagadas ou editadas. A ata notarial pode atestar a veracidade da conversa, porém o tabelião pode atestar um dado falso intencionalmente ou por erro. A perícia no celular pela extração de dados também é uma possibilidade, mas depende da preservação do conteúdo no aparelho para possibilitar sindicância dos elementos de prova, tornando-a vulnerável a inúmeros fatores. (Mota; Freitag, 2023, p. 39-43)

Neste contexto, a *blockchain* se torna a melhor opção para garantir a confiabilidade das provas digitais, como conversas de *WhatsApp*. Isso porque a tecnologia coleta a “impressão digital” do documento e registra em um banco de dados imutável, cuja autenticidade é facilmente verificada através do código *hash*. Portanto, não há motivos razoáveis para deixar de aplicar a tecnologia para garantir a confiabilidade da prova digital no processo penal.

Inclusive, o Superior Tribunal de Justiça reconhece a importância de utilizar a *blockchain* para preservar a cadeia de custódia da prova digital, cuja integridade é mais vulnerável. Vejamos:

- [...] 1. O instituto da cadeia de custódia visa a garantir que o tratamento dos elementos probatórios, desde sua arrecadação até a análise pela autoridade judicial, seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova.
2. Diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, imprescindível se faz a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios, de forma que seja possível a constatação de eventuais alterações, intencionais ou não, dos elementos inicialmente coletados, demonstrando-se a higidez do caminho percorrido pelo material.
3. A auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade são quatro aspectos essenciais das evidências digitais, os quais buscam ser garantidos pela utilização de metodologias e procedimentos certificados, como, e.g., os recomendados pela ABNT.
4. A observação do princípio da mesmidade visa a assegurar a confiabilidade da prova, a fim de que seja possível se verificar a correspondência entre aquilo que foi colhido e o que resultou de todo o processo de extração da prova de seu substrato digital. Uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algoritmo *hash*, a qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos dados do arquivo digital.
5. De relevo trazer à baila o entendimento majoritário desta Quinta Turma no sentido de que "é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia" (AgRg no RHC n. 143.169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, DJe de 2/3/2023).
6. Neste caso, não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do celular apreendido. Logo, evidentes o prejuízo causado pela quebra da cadeia de custódia e a imprestabilidade da prova digital.
7. Agravo regimental provido a fim de conceder a ordem de ofício para que sejam declaradas inadmissíveis as provas decorrentes da extração de dados do celular do corréu, bem como as delas decorrentes, devendo o Juízo singular avaliar a existência de demais elementos probatórios que sustentem a manutenção da condenação. (Brasil, AGRG NO HC N 828.054/RN, 2024)

O precedente acima evidencia a necessidade de utilizar a *blockchain* para preservar a

cadeia de custódia. A tecnologia é acessível e eficaz para garantir a confiabilidade das provas digitais, como conversas no *WhatsApp*. Por essas razões, a *blockchain* deve ser exigida como pressuposto de validade das provas digitais produzidas pela acusação. Isso evita condenações baseadas em provas falsas, efetivando o princípio da presunção de inocência enquanto mecanismo de controle da suficiência probatória.

## **5 A BLOCKCHAIN COMO FERRAMENTA ESSENCIAL À INVESTIGAÇÃO DEFENSIVA.**

A utilidade da *blockchain* não se esgota como garantia de confiabilidade das provas digitais produzidas pelo Ministério Público, demonstrando-se também como ferramenta essencial à investigação defensiva. O Provimento nº 188 de 2018 do Conselho Federal da OAB regulamenta o exercício da investigação defensiva pelo advogado e possibilita a atividade desde a etapa da investigação preliminar até a preparação de revisão preliminar. Além disso, exemplifica diligência investigatórias e expressa o dever profissional de se respeitar os direitos fundamentais dos envolvidos. (CFOAB, 2018)

Segundo BULHÕES (2019, p. 70-73), com a regulamentação administrativa da investigação defensiva pelo Conselho Federal da OAB, surgiu um novo paradigma na advocacia criminal brasileira. Não obstante a viabilidade da investigação defensiva possuir fundamento numa leitura conjunta e harmônica de dispositivos legais e constitucionais, fora a consagração do instituto no direito comparado, o ato normativo veiculou uma ruptura no sistema de justiça criminal doméstico, expulsando parcela considerável das resistências em face do manejo de técnicas de investigação pela advocacia criminal.

Pensando a investigação defensiva dentro da lógica de um sistema acusatório de processo penal, a gestão probatória pertence às partes, devendo o juiz atuar como um garantidor da legalidade processual. Nessa perspectiva, o princípio da paridade de armas veda a existência de uma relação desigual entre as partes. Essa relação de simetria permite à defesa produzir provas para embasar a suas teses, inclusive na fase preliminar. Ao contrário do mito existente, a autoridade que preside a investigação não é responsável por colher todas as provas que servem ao esclarecimento do fato. (Pozzebon; camargo, 2020, p. 22-23).

Assim, somente haverá um contraditório efetivo se possibilitado à defesa técnica uma participação ativa durante toda a persecução penal, de modo que é necessário assegurar o direito à prova numa relação simétrica com a acusação. Contudo, existe um desequilíbrio natural entre acusação e defesa no que tange à capacidade de produção probatória. O Estado-acusação conta com inúmeros meios para produzir provas, enquanto a defesa possui ferramentas limitadas. Se não fosse suficiente, as provas produzidas na investigação criminal oficial tendem a possuir um viés que desfavorece o acusado. (Pedrosa, 2019, p. 50)

Nesse contexto, a investigação defensiva assume a função de reduzir o desequilíbrio existente entre acusação e defesa no que tange à capacidade de produção probatória. Para isso, não basta a paridade de armas estar presente somente na fase judicial, devendo se assegurar a produção probatória pela defesa técnica desde a fase investigativa, pois é neste momento em que os elementos de convicção tendem a ser obtidas de forma mais cristalina. Além do mais, os elementos pela investigação preliminar são replicados massivamente pela acusação na fase judicial, evidenciando a relevância do momento antecedente na resolução do caso penal. (Penedo, 2018, p. 297)

Durante a investigação preliminar, é possível que o investigado indique a produção de uma prova que a autoridade policial, ou o presidente da investigação oficial, não tenha o interesse ou não seja diligente em produzir. Assim, é fundamental conceder à defesa técnica um papel ativo na produção probatória, sob pena de se perder a oportunidade de esclarecer um fato relevante que poderia impactar significativamente o resultado da persecução penal.

Nesse contexto, em se tratando de provas digitais, a defesa técnica pode empregar a

tecnologia *blockchain* para coletar essas evidências de forma independente, isto é, sem depender da vontade ou diligência da autoridade policial em produzi-las. Existem diversas ferramentas disponíveis que fazem uso da tecnologia *blockchain* para preservar a prova digital:

No Brasil foram usados num processo penal meios de prova armazenados na *blockchain*, nomeadamente publicações de redes sociais como o Facebook, Instagram e Twitter. Através do projeto da OriginalMy o autor providenciou a preservação de todo o conteúdo das provas na plataforma Blockchain, para que as ofensas que circulavam nas redes sociais pudessem ser removidas sem que tal prejudicasse o processo penal. A introdução numa *blockchain* foi uma forma de comprovar a veracidade e a existência daquelas publicações sem prejudicar a justiça. A OriginalMy usa a extensão PACWeb que, quando instalada no navegador, gera automaticamente um relatório em formato PDF daquilo que se está a visualizar, sejam mensagens no Telegram, Whatsapp, Facebook, email; além do relatório também grava em vídeo o mesmo conteúdo. De seguida os dados são inseridos numa *blockchain* para se comprovar que a prova não sofreu alterações e mesmo se o conteúdo for eliminado da internet, há esse registo com a hora e data em que ocorreu. Outro projeto que se dedica à conservação de provas para a sua posterior utilização no processo é a plataforma HashCool que tem como finalidade o registo de documentos e arquivos digitais ou digitalizados, assim como informações contidas em URL's, garantindo a sua imutabilidade e autenticidade. Por fim, o UProof é um serviço que certifica fotos, vídeos ou ficheiros de áudio com data e hora para que sejam considerados autênticos; após ser criada uma chave com indicação da hora e data, é inserida na *blockchain* e há um bloqueio daquele ficheiro, que caso seja alterado, caso ocorra a alteração de um simples pixel, a chave criada no início já não corresponderá à criada posteriormente à modificação. (Hermeiro, 2023, p. 49)

Portanto, a *blockchain* surge como uma ferramenta essencial para a investigação defensiva, permitindo que a defesa técnica colete e preserve provas digitais de forma independente, sem depender exclusivamente das investigações realizadas pela acusação. Isso reduz o desequilíbrio entre acusação e defesa, garantindo que ambas as partes tenham acesso às mesmas oportunidades de produção probatória. Assim, a tecnologia *blockchain*, além de promover a confiabilidade das provas digitais, também fortalece os princípios do contraditório, paridade de armas e ampla defesa, essenciais para a decisão justa no processo penal.

## 6 CONCLUSÃO

Diante do exposto, é inegável que o advento das novas tecnologias implica desafios complexos e multifacetados para o sistema judicial, especialmente no que diz respeito à produção, coleta e confiabilidade das provas digitais no processo penal. Vivemos em uma sociedade profundamente imersa na era digital, onde as interações e transações ocorrem cada vez mais por meio de dispositivos eletrônicos e plataformas online. Nesse cenário, a crescente digitalização não apenas facilita a comunicação e o acesso à informação, mas também traz consigo implicações significativas para a administração da justiça e para a proteção dos direitos individuais.

A proliferação de crimes cibernéticos e a disseminação de evidências digitais, como mensagens de texto, e-mails, registros de transações financeiras e mídias digitais, ampliam exponencialmente a complexidade do processo de investigação e julgamento. A confiabilidade e a integridade dessas provas são fundamentais para a garantia de uma decisão justa no processo penal. No entanto, a natureza volátil e facilmente manipulável das informações digitais representa um desafio significativo para os sistemas tradicionais de coleta e apresentação de provas, demandando abordagens inovadoras e adaptativas por parte do sistema judiciário.

Nesse contexto, a tecnologia *blockchain* emerge como uma solução inovadora e promissora para endereçar esses desafios de forma eficaz. Ao oferecer um registro distribuído e imutável de transações e informações digitais, a *blockchain* proporciona uma camada adicional de

segurança e confiabilidade, tornando extremamente difícil a adulteração ou falsificação das evidências. Através da criptografia e da descentralização, a integridade dos dados é garantida, conferindo maior credibilidade aos elementos probatórios apresentados durante no processo penal.

Além disso, a *blockchain* oferece uma gama de oportunidades na investigação defensiva, permitindo que a defesa colete e preserve provas digitais de forma independente e transparente. Isso equilibra a relação entre acusação e defesa, garantindo que ambas as partes tenham acesso às mesmas oportunidades de produção probatória.

Portanto, frente aos desafios impostos pela era digital, a adoção efetiva e generalizada da tecnologia *blockchain* torna-se não apenas uma opção viável, mas uma necessidade imperativa para garantir a eficácia e a legitimidade do sistema de justiça. É fundamental que os atores processuais se adaptem e incorporem essas inovações de forma proativa, assegurando assim uma administração da justiça moderna, eficiente, transparente e verdadeiramente equitativa, que respeite os direitos fundamentais. Esta adaptação não apenas fortalece a confiança da sociedade no sistema de justiça, mas também contribui para o aprimoramento contínuo das instituições democráticas e para a consolidação do Estado de Direito. Em última análise, a integração da tecnologia *blockchain* no âmbito jurídico não se limita a uma mera questão técnica, mas representa um marco significativo na evolução do sistema de justiça, marcando o início de uma nova era de transparência, eficiência e justiça para todos.

## REFERÊNCIAS

BADARÓ, Gustavo Henrique Righi Ivahy. **A cadeia de custódia da prova digital**. In: OSNA, Gustavo et. al (org.). *Direito probatório*. Londrina: Thoth, 2023, p. 175-188.

BADARÓ, Gustavo Henrique. **Epistemologia judiciária e prova penal**. São Paulo: Thomson Reuters Brasil, 2019.

BELTRÁN, Jordi Ferrer. La prueba es libertad, pero no tanto: una teoría de la prueba cuasi-benthamiana. **Revista Jurídica Mario Alario D’Filippo**, Cartagena (Colombia), v. 9, n. 18, p. 150-169, jul./dez. 2017.

BARREIRA, Wagner. Era da informação: tudo ao mesmo tempo agora. **Superinteressante**, São Paulo, 31 ago. 1994. Disponível em: <https://cutt.ly/7eqHV8xL>. Acesso em: 29 abr. 2024.

BRANDÃO, Cláudio. **Teoria Jurídica do Crime**. 6. ed. Belo Horizonte: D’Plácido, 2022.

BRASIL. Conselho Nacional de Justiça. **Resolução CNJ nº 345, de 9/10/2020**. Dispõe sobre o “Juízo 100% Digital” e dá outras providências. Brasília, DF: 9 out. 2020a. Disponível em: <https://cutt.ly/PeqHBpSa>. Acesso em: 29 abr. 2024.

BRASIL. Conselho Nacional de Justiça. **Resolução CNJ nº 484, de 19/12/2022**. Estabelece diretrizes para a realização do reconhecimento de pessoas em procedimentos e processos criminais e sua avaliação no âmbito do Poder Judiciário. Brasília, DF: 19 dez. 2022. Disponível em: <https://cutt.ly/heqHBYDx>. Acesso em: 29 abr. 2024.

BRASIL. Convenção sobre o Crime Cibernético (2001). **Decreto nº 11.491 de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023. Disponível em: <https://cutt.ly/Seqk4RTE>. Acesso em: 29 abr. 2024.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo Regimental no Habeas Corpus**

**828.054/RN. PROCESSUAL PENAL. AGRAVO REGIMENTAL NO HABEAS CORPUS. TRÁFICO DE DROGAS. APREENSÃO DE CELULAR. EXTRAÇÃO DE DADOS. CAPTURA DE TELAS. QUEBRA DA CADEIA DE CUSTÓDIA. INADMISSIBILIDADE DA PROVA DIGITAL. [...].** Relator: Min. Joel Ilan Paciornik, 23 abr. 2024. Brasília: STJ, 2024. Disponível em: <https://cutt.ly/HeqHNu2B>. Acesso em: 29 abr. 2024.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 598.886/SC. HABEAS CORPUS. ROUBO MAJORADO. RECONHECIMENTO FOTOGRÁFICO DE PESSOA REALIZADO NA FASE DO INQUÉRITO POLICIAL. INOBSERVÂNCIA DO PROCEDIMENTO PREVISTO NO ART. 226 DO CPP. PROVA INVÁLIDA COMO FUNDAMENTO PARA A CONDENAÇÃO. RIGOR PROBATÓRIO. NECESSIDADE PARA EVITAR ERROS JUDICIÁRIOS. PARTICIPAÇÃO DE MENOR IMPORTÂNCIA. NÃO OCORRÊNCIA. ORDEM PARCIALMENTE CONCEDIDA. [...].** Relator: Min. Rogério Schietti Cruz, 27 out. 2020. Brasília: STJ, 2020b. Disponível em: <https://cutt.ly/7eqlqYEE>. Acesso em: 29 abr. 2024.

BULHÕES, Gabriel. **Manual prático de investigação defensiva: um novo paradigma na advocacia criminal brasileira.** Florianópolis: EMais, 2019.

CIDRÃO, Taís Vasconcelos; MUNIZ, Antônio Walber; ALVES, Ana Abigail Costa Vasconcelos. A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da Convenção de Budapeste à legislação brasileira, **Brazilian Journal of International Relations**, Marília, SP, v. 7, n. 1, p. 66–82, 2018. Disponível em: <https://cutt.ly/3eqHNDbU>. Acesso em: 29 abr. 2024.

CORTE IDH. **Ruano Torres y otros vs. El Salvador.** 05 out. 2015. Disponível em: <https://cutt.ly/5jncNQx>. Acesso em: 29 abr. 2024.

DAVID, Décio Franco; MINSKI, Bruno Henrique Zanette. Blockchain como mecanismo de criminal compliance à luz da Lei 13.709/2018. **Revista de Direito Penal Econômico e Compliance.** n. 5. ano 2. p. 71-97. São Paulo: Ed. RT, jan./mar. 2021.

FERRAJOLI, Luigi. **Direito e razão: Teoria do garantismo penal.** 3. ed. São Paulo: Editora Revistas dos Tribunais, 2022.

GOOGLE. **Linha do tempo do Google Maps.** 20---. Disponível em: <https://cutt.ly/Feqk4SN0>. Acesso em: 29 abr. 2024.

GLOBO. **Denúncias de crimes cometidos pela internet mais que dobram em 2020.** Portal G1, 9 fev. 2021a. Disponível em: <https://cutt.ly/9eqHMqep>. Acesso em: 29 abr. 2024.

GLOBO. **PM em Juiz de Fora impede estupro durante monitoramento de câmeras do 'Olho Vivo'.** Portal do G1, 19 mai. 2021b. Disponível em: <https://cutt.ly/ueqk4OHx>. Acesso em: 29 abr. 2024.

HERMEIRO, Andreia Carina Cláudio. **A cadeia de custódia da prova digital: O uso da tecnologia Blockchain como forma de preservação.** 2023. Dissertação (Mestrado em Direito) - 2023. Universidade de Coimbra, Coimbra, 2023. Disponível em: <https://cutt.ly/ReqHMTLX>. Acesso em: 01 mai. 2024.

LEITE, Vitor. **O que é blockchain**: uma explicação simples. Blog Nubank, 05 out. 2020. Disponível em: <https://cutt.ly/NeqHM4JC>. Acesso em: 18 mai. 2021.

LOPES Jr., Aury. **Direito Processual Penal**. 17. ed. São Paulo: Saraiva, 2020.

MOTTA, Débora; FREITAG, Leandro Ernani. Provas Digitais e o Problema do Print Screen. **Revista da ESMESC**, Santa Catarina, v. 30, n. 36, p. 24-50, dez. 2023. Disponível em: <https://cutt.ly/EeqH1sIP>. Acesso em: 29. abr. 2024.

NAKAMOTO, Satoshi. **Bitcoin**: A Peer-to-Peer Electronic Cash System. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 29 abr. 2024.

NARDELLI, Marcella Alves Mascarenhas. Presunção de Inocência, Standards de Prova e Racionalidade das Decisões sobre os Fatos no Processo Penal. In: SANTORO, Antônio Eduardo Ramires; MALAN, Diogo Rudge; MADURO, Flávio Mirza (org.). **Crise no processo penal contemporâneo**: escritos em homenagem aos 30 anos da Constituição de 1988. Belo Horizonte: D'Plácido, 2018.

NUNES, Dierle. Virada tecnológica no direito processual (da automação à transformação): seria possível adaptar o procedimento pela tecnologia. In: NUNES, Dierle; LUCON, Pedro Henrique dos Santos; WOLKART, Erika Navarro. **Inteligência Artificial e Direito Processual**: os impactos da virada tecnológica no direito processual. Salvador: Editora JusPodivm, 2020.

CFOAB. Conselho Federal da Ordem dos Advogados do Brasil. **Provimento N° 188/2018**. Regulamenta o exercício da prerrogativa profissional do advogado de realização de diligências investigatórias para instrução em procedimentos administrativos e judiciais. Brasília, DF: 11 dez. 2018. Disponível em: <https://cutt.ly/veqIQJzt>. Acesso em: 29 abr. 2024.

PEDROSA, Simon Francisco. Investigação Defensiva. **Revista do CAAP**, Belo Horizonte, v. 29, n. 2, p. 47-72, 2019. Disponível em: <https://cutt.ly/XeqH0yRS>. Acesso em: <https://acesse.dev/Mb7yz>.

PENEDO, Larissa Gomes. Investigação criminal defensiva: a atuação ativa da defesa na fase pré-processual e busca pela paridade de armas. **Revista da Defensoria Pública do Estado do Rio Grande do Sul**, Porto Alegre, n. 27, p. 288–306, 2021. Disponível em: <https://cutt.ly/seqH0ULk>. Acesso em: 29. abr. 2024.

PINHEIRO, Reginaldo César. Os crimes virtuais na esfera jurídica brasileira. **Boletim do IBCCRIM**, São Paulo, n. 101, p. 18-19, abr. 2001.

POZZEBON, Fabricio Dreyer de Ávila; CAMARGO, Rodrigo Oliveira de. A relevância do juiz das garantias para a investigação defensiva na fase preliminar. **Boletim do IBCCRIM**, São Paulo, n. 334, p. 21-23, set. 2020.

PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. **Consultor Jurídico**, São Paulo, 21 jan. 2021. Disponível em: <https://cutt.ly/oeqH06aD>. Acesso em: 29 abr. 2024.

ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a Teoria dos jogos e MCDA-A. 1. ed. Florianópolis: Emais, 2021.

ROSA, Alexandre Morais da; RUDOLFO, Fernanda Mambrini. A teoria da perda de uma chance probatória aplicada ao processo penal. **Revista Brasileira de Direito**, Passo Fundo, v. 13, n. 3, p. 455-471, dez. 2017.

SIMANTOB, Fábio Tofic. Delitos virtuais: o lugar do crime na visão dos tribunais. **Revista do Advogado**, São Paulo, v. 32, n. 115, p. 61-68, abr. 2012.

SOMBRIO, Débora Normanton. Nem tudo é prova: a cadeia de custódia como método de controle de fixação dos fatos no processo penal. In: SARKIS, Jamila Monteiro; NETO, José de Assis Santiago; PAULA, Leonardo Costa de. **Tudo e mais um pouco da inquisitorialidade no processo penal**: Estudos em homenagem ao Professor Leonardo Marinho. Curitiba: Observatório da Mentalidade Inquisitória, 2021. p. 199-224.

SUSSKIND, Richard. **Online Courts and the Future of Justice**. New York: Oxford University Press, 2019.