Cadeia de custódia e prova digital: Garantismo e jurisprudência

Washington Ramos Monteiro

1. INTRODUÇÃO.

A transição para uma sociedade hiperconectada reconfigurou não apenas as relações sociais e econômicas, mas também a fenomenologia do crime e os métodos de investigação criminal. No cenário contemporâneo, a prova digital deixou de ser um elemento acessório para se tornar o eixo central de grande parte das investigações penais, desde crimes cibernéticos propriamente ditos até delitos tradicionais como tráfico de drogas, corrupção e crimes contra a vida, onde a comunicação via aplicativos e o rastro digital de geolocalização fornecem evidências cruciais.

Entretanto, a natureza técnica da prova digital marcada pela volatilidade, facilidade de alteração e invisibilidade de manipulações para o olho não treinado impõe ao Direito Processual Penal a necessidade de um rigor metodológico sem precedentes. É nesse contexto que a cadeia de custódia emerge como o instituto jurídico-processual destinado a garantir a autenticidade e a integridade dos vestígios digitais, assegurando que a prova valorada pelo magistrado seja idêntica àquela coletada na cena do crime ou no dispositivo eletrônico.

Sob a ótica de Luigi Ferrajoli, a legitimidade da punição estatal depende estritamente da observância de formas processuais que limitem o arbítrio e garantam o direito de defesa. A cadeia de custódia, portanto, não deve ser vista como um entrave burocrático à eficácia investigativa, mas como uma condição de validade epistêmica da prova. Sem a garantia de que a evidência não foi manipulada, o processo penal perde sua racionalidade e se aproxima de um modelo autoritário de "verdade a qualquer preço".

Este trabalho propõe-se a analisar a evolução desse instituto no Brasil, especialmente após a positivação da cadeia de custódia pelo Pacote Anticrime em 2019. O estudo dedica especial atenção à jurisprudência do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF) entre os anos de 2020 e 2025, período em que os tribunais foram confrontados com dilemas complexos envolvendo mensagens de WhatsApp, espelhamento de dados e o uso de tecnologias de vigilância em massa. Através de uma abordagem crítica e garantista, busca-se demonstrar que o rigor na preservação da prova digital é o único caminho para um processo penal que respeite a dignidade da pessoa humana e os princípios democráticos.

2. FUNDAMENTOS TEÓRICOS E GARANTISMO PENAL NA ERA DIGITAL

2.1 O Garantismo Jurídico de Luigi Ferrajoli: Limites ao Poder Punitivo

O garantismo jurídico, conforme delineado por Luigi Ferrajoli em sua obra monumental *Diritto e Ragione*, não é apenas uma teoria do direito penal, mas uma filosofia política de limitação do poder. Ferrajoli propõe um modelo de "Direito Penal Mínimo", onde

a intervenção estatal é justificada apenas quando estritamente necessária para a proteção de bens jurídicos fundamentais e sempre subordinada a um sistema rígido de garantias.

No coração do garantismo está a ideia de que o poder punitivo é, por natureza, uma força potencialmente arbitrária e violenta. Para neutralizar essa tendência, o sistema jurídico deve impor "vínculos de validade" que condicionam o exercício do poder à observância de regras formais e substanciais. Ferrajoli articula dez axiomas que formam o sistema garantista (como *nulla poena sine crimine*, *nullum crimen sine lege*, *nulla lex poenalis sine necessitate*, entre outros), culminando no axioma *nulla probatio sine defensione* não há prova sem defesa.

Na era digital, esses limites tornam-se ainda mais vitais. A tecnologia conferiu ao Estado capacidades de vigilância e coleta de dados que Ferrajoli dificilmente poderia prever em 1989. O garantismo, portanto, deve ser atualizado para enfrentar o "panoptismo digital", onde a facilidade de obtenção de dados eletrônicos pode levar a um relaxamento das formas processuais em nome de uma suposta eficiência. A defesa das garantias individuais contra o arbítrio tecnológico é a nova fronteira do garantismo penal.

2.2 A Verdade Processual como Verdade Aproximada e Controlável

Um dos pontos mais profundos da teoria de Ferrajoli é a desconstrução da "verdade substancial" ou "verdade real". Para o garantismo, a busca por uma verdade absoluta no processo penal é uma ilusão metafísica que historicamente serviu para justificar a tortura e o autoritarismo. Em seu lugar, Ferrajoli propõe a verdade processual, que é uma verdade aproximada, obtida através de um método racional e controlável.

A verdade processual é "verdade" apenas na medida em que é verificável e falsificável através do contraditório. Ela não é o que "realmente aconteceu", mas o que pode ser provado seguindo as regras do jogo processual. Michele Taruffo, em diálogo com essa perspectiva, ressalta que a prova é um instrumento de conhecimento que deve seguir padrões de racionalidade e probabilidade lógica.

No âmbito da prova digital, essa distinção é crucial. Um arquivo digital, por si só, não é a "verdade". Ele é um vestígio que precisa ter sua origem, integridade e contexto verificados. A cadeia de custódia é, precisamente, o mecanismo que permite o controle epistêmico sobre a prova digital. Se a cadeia é quebrada, a "controlabilidade" da prova desaparece, e qualquer conclusão baseada nela torna-se um ato de fé, não de razão jurídica.

2.3 O Devido Processo Legal e a Presunção de Inocência na Produção da Prova

O devido processo legal (*due process of law*) e a presunção de inocência são os pilares que sustentam a produção probatória em um Estado Democrático de Direito. A presunção de inocência, como regra de tratamento e regra de prova, impõe que o ônus de demonstrar a culpa recaia inteiramente sobre a acusação. Mais do que isso, exige que a prova apresentada seja robusta o suficiente para superar qualquer dúvida razoável (*standard* de prova *beyond a reasonable doubt*).

A produção da prova, portanto, deve ser um processo dialético. O contraditório não é apenas o direito de falar após a acusação, mas o direito de participar ativamente da

construção do material probatório. Na prova digital, isso implica o direito da defesa de acessar as mídias originais, de examinar os metadados e de realizar sua própria perícia.

Quando o Estado coleta uma prova digital e não preserva sua cadeia de custódia, ele está, na prática, cerceando a defesa e violando a presunção de inocência. Uma prova cuja integridade não pode ser verificada é uma prova que não pode ser contestada de forma efetiva. O garantismo exige que a paridade de armas seja mantida mesmo diante da complexidade técnica da informática forense.

2.4 A Prova Ilícita e a Teoria dos Frutos da Árvore Envenenada

A inadmissibilidade das provas ilícitas é uma garantia constitucional (Art. 5º, LVI, CF/88) que atua como um freio ético à atividade estatal. Prova ilícita é aquela obtida com violação de direitos fundamentais. No contexto digital, isso ocorre frequentemente em acessos a dispositivos sem autorização judicial, quebras de sigilo de dados sem fundamentação adequada ou interceptações de comunicações que extrapolam os limites legais.

A teoria dos frutos da árvore envenenada (*fruits of the poisonous tree*), acolhida pelo ordenamento brasileiro, estabelece que a ilicitude de uma prova se comunica a todas as provas dela derivadas. Se a coleta inicial de um rastro digital foi ilícita, todo o desdobramento investigativo baseado nela está contaminado.

A quebra da cadeia de custódia, embora muitas vezes tratada como uma irregularidade formal, pode atingir o patamar da ilicitude quando impede a verificação da autenticidade da prova. Se o Estado apresenta um dado digital e não pode provar que ele não foi manipulado, ele está apresentando uma prova cuja confiabilidade é nula. Sob uma ótica garantista estrita, a impossibilidade de verificação da integridade equivale à inexistência de prova lícita, pois a dúvida sobre a manipulação deve sempre favorecer o acusado.

3. CAPÍTULO II: A PROVA DIGITAL E OS DESAFIOS DA INFORMÁTICA FOREN

3.1 Conceito, Natureza e Classificação das Provas Digitais

A prova digital, também conhecida como evidência eletrônica ou forense digital, é definida como qualquer informação de valor probatório armazenada ou transmitida em formato digital. Sua natureza intangível e a forma como é gerada, armazenada e processada a distinguem das provas materiais tradicionais. Não se trata apenas de um documento digitalizado, mas de dados que, por sua própria essência, existem no ambiente eletrônico, como e-mails, mensagens de aplicativos, registros de acesso, metadados, arquivos de log, imagens e vídeos digitais, dados de geolocalização, entre outros.

A doutrina tem se esforçado para classificar as provas digitais, geralmente distinguindo-as pela sua origem ou pelo seu tipo. Uma classificação útil as divide em: (i) dados de comunicação, que incluem o conteúdo de mensagens, e-mails e chamadas; (ii) dados de tráfego, que revelam informações sobre a comunicação (quem, quando, onde, como), mas não o conteúdo; (iii) dados de localização, que indicam a posição geográfica de um dispositivo ou usuário; e (iv) dados de conteúdo armazenado, que são arquivos diversos

(documentos, fotos, vídeos) em dispositivos ou na nuvem. Essa categorização é fundamental para a aplicação das normas processuais e constitucionais que regem a privacidade e o sigilo.

3.2 Características da Prova Digital: Volatilidade, Mutabilidade e Fragilidade

As provas digitais possuem características intrínsecas que as tornam particularmente desafiadoras para o sistema de justiça criminal, exigindo protocolos específicos para sua coleta e preservação. As principais são:

Volatilidade: Dados digitais podem ser facilmente perdidos ou alterados com o tempo, com o desligamento de um dispositivo, ou mesmo com a simples operação de um sistema. Informações na memória RAM, por exemplo, são extremamente voláteis e exigem coleta imediata.

Mutabilidade: A facilidade de alteração é uma das maiores preocupações. Um arquivo de texto, uma imagem ou uma mensagem podem ser modificados sem deixar rastros evidentes para um observador comum. A data e hora de criação ou modificação também podem ser alteradas.

Fragilidade: A prova digital é suscetível a danos acidentais ou intencionais. Um dispositivo pode ser danificado fisicamente, um arquivo pode ser corrompido, ou um sistema pode ser invadido e ter seus dados apagados ou alterados.

Ubiquidade: Dados podem estar armazenados em múltiplos locais (dispositivos locais, servidores remotos, nuvem), dificultando o isolamento e a coleta completa.

Invisibilidade: Muitos dados relevantes (metadados, arquivos deletados, fragmentos de arquivos) não são visíveis para o usuário comum, exigindo ferramentas e técnicas forenses para sua recuperação.

Essas características ressaltam a necessidade de uma abordagem técnica especializada e de um rigoroso controle da cadeia de custódia para garantir que a prova digital mantenha sua integridade e autenticidade desde o momento da sua identificação até a sua apresentação em juízo. A ausência de tais cuidados pode levar à contaminação da prova, tornando-a imprestável para o processo penal.

3.3 Standards Técnicos Internacionais: A ISO/IEC 27037 e a Perícia Forense

Diante da complexidade e das características peculiares da prova digital, a informática forense desenvolveu metodologias e *standards* internacionais para assegurar a integridade e a autenticidade das evidências eletrônicas. A norma ISO/IEC 27037:2012 (Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital) é um dos principais referenciais nesse campo.

Esta norma estabelece diretrizes para as fases iniciais da manipulação da evidência digital, desde a sua identificação no local do crime até a sua preparação para análise forense. Ela enfatiza a importância de:

Identificação: Reconhecer potenciais fontes de evidência digital.

Coleta: Obter a evidência de forma a preservar sua integridade, utilizando métodos como a criação de imagens forenses (bit-a-bit) de discos rígidos e dispositivos móveis.

Aquisição: Transferir a evidência para um meio de armazenamento seguro, garantindo que o original não seja alterado.

Preservação: Manter a evidência em condições que evitem sua alteração, perda ou contaminação, documentando todas as ações realizadas.

A aplicação desses *standards* técnicos é crucial para a validade da prova digital. A utilização de *hash* (funções criptográficas que geram um "resumo" único de um arquivo) é um exemplo de técnica forense que permite verificar se um arquivo foi alterado. Se o *hash* do arquivo original for diferente do *hash* do arquivo apresentado em juízo, há uma forte indicação de que a prova foi adulterada, comprometendo sua autenticidade.

3.4 O Desafio da Prova em Nuvem e a Criptografia de Ponta a Ponta

Com a crescente popularidade dos serviços de computação em nuvem (*cloud computing*) e a utilização de aplicativos de comunicação com criptografia de ponta a ponta, a obtenção e a preservação da prova digital enfrentam novos e complexos desafios. Dados armazenados em nuvem não estão fisicamente em um dispositivo, mas em servidores remotos, muitas vezes em diferentes jurisdições, o que levanta questões sobre competência, cooperação jurídica internacional e a aplicabilidade de mandados judiciais.

A criptografia de ponta a ponta, utilizada por aplicativos como WhatsApp e Telegram, garante que apenas o remetente e o destinatário possam ler as mensagens, tornando-as inacessíveis até mesmo para os provedores do serviço. Isso representa um dilema para as autoridades investigativas, que buscam acesso ao conteúdo das comunicações para fins de prova. A quebra dessa criptografia, sem o consentimento dos usuários ou uma ordem judicial específica e fundamentada, pode configurar grave violação de direitos fundamentais, como a privacidade e o sigilo das comunicações.

Nesse cenário, a informática forense e o direito precisam desenvolver novas abordagens. A obtenção de dados diretamente dos dispositivos dos investigados, com autorização judicial, ou a cooperação com provedores de serviços para acesso a metadados (que não são criptografados) tornam-se alternativas. Contudo, a tensão entre a necessidade de investigação e a proteção da privacidade digital permanece como um dos maiores desafios para o garantismo penal na era da nuvem e da criptografia.

4. A CADEIA DE CUSTÓDIA COMO GARANTIA EPISTÊMICA E PROCESSUAL

4.1 Evolução Legislativa: O Pacote Anticrime e os Arts. 158-A a 158-F do CPP

A cadeia de custódia, embora já reconhecida pela doutrina e jurisprudência como um princípio implícito do devido processo legal, ganhou contornos legislativos explícitos no Brasil com a promulgação da Lei nº 13.964/2019, conhecida como "Pacote Anticrime". Esta lei inseriu os artigos 158-A a 158-F no Código de Processo Penal (CPP), dedicando uma seção inteira à disciplina da cadeia de custódia.

O art. 158-A do CPP define cadeia de custódia como "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte". Essa definição legal é abrangente e aplica-se a qualquer tipo de vestígio, incluindo, por óbvio, os vestígios digitais. A lei estabelece, portanto, um marco formal para a garantia da integridade da prova, que antes dependia da interpretação judicial e da aplicação analógica de normas.

A positivação da cadeia de custódia representa um avanço significativo para o garantismo penal. Ao detalhar as etapas e a necessidade de documentação, a lei busca reduzir a discricionariedade dos agentes estatais na coleta e manuseio da prova, impondo um controle formal que visa a proteger o acusado contra a manipulação ou contaminação das evidências. É um reconhecimento legislativo da importância da integridade da prova para a legitimidade do processo penal.

4.2 As Etapas da Cadeia de Custódia: Do Reconhecimento ao Descarte

Os artigos 158-B e 158-C do CPP detalham as etapas da cadeia de custódia, que devem ser rigorosamente observadas para garantir a integridade do vestígio. Embora a lei não se refira especificamente à prova digital, seus princípios são perfeitamente aplicáveis e, em muitos casos, ainda mais cruciais devido à volatilidade e mutabilidade dos dados eletrônicos. As etapas são:

Reconhecimento: Ato de constatar a existência de um vestígio. No contexto digital, pode ser a identificação de um dispositivo eletrônico, um registro de log ou uma mensagem em uma plataforma.

Isolamento: Preservar o local ou o objeto onde o vestígio foi encontrado, evitando alterações. Para a prova digital, isso pode significar desligar um computador da rede, isolar um celular em um saco Faraday ou congelar o estado de um servidor.

Fixação: Descrever e documentar o vestígio e o local onde foi encontrado. Na prova digital, isso envolve a documentação fotográfica, a descrição detalhada do dispositivo, a criação de um *hash* do arquivo.

Coleta: Recolher o vestígio, observando as técnicas forenses adequadas. Para dados digitais, a coleta deve ser feita por meio de cópias forenses bit-a-bit, garantindo que o original não seja alterado e que todos os metadados sejam preservados.

Acondicionamento: Embalar o vestígio de forma a preservar suas características. Dispositivos eletrônicos devem ser acondicionados em embalagens antiestáticas e lacrados, com informações sobre a coleta.

Transporte: Mover o vestígio do local da coleta para o local da perícia ou armazenamento, garantindo que não haja alteração ou contaminação.

Recebimento: Documentar a entrega do vestígio no local de destino, com registro de quem recebeu, quando e em que condições.

Processamento: A análise pericial do vestígio. Na informática forense, envolve a extração de dados, a recuperação de arquivos deletados, a análise de metadados, entre outros procedimentos.

Armazenamento: Guardar o vestígio em local seguro e adequado, com controle de acesso e registro de todas as movimentações.

Descarte: Destinação final do vestígio após o término do processo, conforme a legislação e as normas ambientais.

Cada uma dessas etapas deve ser documentada de forma minuciosa, com registros de data, hora, local, quem realizou a ação e quais procedimentos foram adotados. A falha em qualquer uma dessas etapas pode comprometer a integridade da prova e, consequentemente, sua validade no processo penal.

4.3 A Quebra da Cadeia de Custódia: Consequências Jurídicas

A quebra da cadeia de custódia ocorre quando há uma falha em qualquer uma das etapas descritas, resultando na perda da rastreabilidade, integridade ou autenticidade do vestígio. No contexto da prova digital, uma quebra pode ser a ausência de um *hash* do arquivo original, a falta de documentação sobre quem acessou um dispositivo, ou a alteração de metadados sem registro.

As consequências jurídicas da quebra da cadeia de custódia são graves e podem levar à inadmissibilidade da prova. O art. 158-D do CPP estabelece que "o recipiente com o vestígio deverá ser selado com lacre, com informações que permitam sua identificação, de modo a garantir a inviolabilidade e idoneidade do material". A violação desse lacre, ou a ausência de sua correta aplicação, pode gerar a nulidade da prova.

Sob a ótica garantista, a quebra da cadeia de custódia não é uma mera irregularidade formal. Ela atinge o cerne da confiabilidade da prova, tornando-a duvidosa. Se não é possível garantir que a prova digital apresentada em juízo é a mesma que foi coletada, sem alterações, ela perde sua capacidade de fundamentar uma decisão judicial justa. A presunção de inocência exige que a acusação prove a culpa além de qualquer dúvida razoável, e uma prova com a cadeia de custódia quebrada não pode satisfazer esse *standard*.

4.4 O Ônus da Prova e a Presunção de Integridade: Uma Crítica Garantista

Um dos debates mais relevantes em torno da cadeia de custódia diz respeito ao ônus da prova da sua quebra e às consequências dessa quebra. Em alguns julgados, tem-se observado uma tendência em exigir que a defesa demonstre o prejuízo concreto ou a efetiva manipulação da prova para que a quebra da cadeia de custódia resulte em nulidade. Essa abordagem, contudo, é alvo de críticas sob uma perspectiva garantista.

Para o garantismo, a presunção de integridade da prova deve ser do Estado. É o órgão acusador que tem o dever de apresentar uma prova cuja autenticidade e integridade sejam inquestionáveis, através da observância rigorosa da cadeia de custódia. Exigir que a defesa prove a manipulação ou o prejuízo é inverter o ônus da prova, colocando sobre o acusado

a tarefa de demonstrar um fato negativo (a não-integridade da prova) que, muitas vezes, é tecnicamente impossível de ser comprovado sem acesso aos meios e conhecimentos que o Estado possui.

Quando a cadeia de custódia é quebrada, a prova digital perde sua confiabilidade intrínseca. A dúvida sobre sua integridade deve, por força da presunção de inocência e do *in dubio pro reo*, operar em favor do acusado. A quebra da cadeia de custódia, portanto, deve gerar a nulidade da prova, independentemente da demonstração de prejuízo concreto, pois o prejuízo é inerente à perda da confiabilidade e à violação do devido processo legal. A prova digital, sem uma cadeia de custódia íntegra, é uma prova ilícita por derivação, pois sua origem e manuseio não podem ser garantidos.

5. ANÁLISE CRÍTICA DA JURISPRUDÊNCIA DOS TRIBUNAIS SUPERIORES (2020-2025)

5.1 O Precedente Histórico: A "Operação Open Doors" (RHC 143.169/RJ)

Um dos marcos mais significativos na jurisprudência brasileira sobre a cadeia de custódia digital é o julgamento do Recurso em Habeas Corpus (RHC) 143.169/RJ pela Sexta Turma do Superior Tribunal de Justiça (STJ), em 2021, no âmbito da "Operação Open Doors". Neste caso, o STJ anulou provas obtidas por meio de espelhamento de mensagens de WhatsApp via WhatsApp Web, sem a observância das formalidades legais e sem a garantia da cadeia de custódia.

A decisão foi paradigmática por reconhecer a fragilidade da prova digital obtida sem os devidos cuidados técnicos e legais. O relator, Ministro Nefi Cordeiro, destacou que a ausência de perícia que atestasse a integridade das mensagens, bem como a falta de documentação sobre o processo de coleta e preservação, comprometia a autenticidade da prova. A Turma entendeu que a simples captura de tela (*print screen*) ou o espelhamento via WhatsApp Web não são suficientes para garantir a imutabilidade do conteúdo, que poderia ser facilmente editado ou manipulado.

Este precedente reforçou a compreensão de que a cadeia de custódia não é uma mera formalidade, mas um requisito essencial para a validade da prova digital, atuando como um filtro garantista contra a arbitrariedade e a manipulação. A decisão do STJ sinaliza a necessidade de um rigoroso controle sobre a forma de obtenção e preservação das evidências digitais, sob pena de nulidade processual.

5.2 Mensagens de WhatsApp: Prints, Espelhamento e Infiltração Virtual (2024-2025)

A questão das mensagens de WhatsApp continua a ser um dos temas mais debatidos na jurisprudência. Em 2024 e 2025, o STJ consolidou entendimentos importantes:

Prints de tela: O STJ tem reiterado que *prints* de tela de conversas de WhatsApp, por si só, não são provas robustas. A facilidade de edição e a ausência de metadados que comprovem a autenticidade tornam-nos frágeis. A validade de tais provas depende de outros elementos que corroborem seu conteúdo e, idealmente, de uma perícia técnica que ateste sua integridade. Em casos de violência doméstica, no entanto, o STJ tem mitigado o

rigor, aceitando *prints* obtidos por particulares quando não há indícios de manipulação e são corroborados por outros elementos de prova, transferindo o ônus de demonstrar o prejuízo ou a manipulação para a defesa.

Espelhamento via WhatsApp Web: Após o precedente da "Operação Open Doors", o STJ tem se posicionado de forma mais cautelosa. Contudo, em abril de 2024, a 5ª Turma do STJ, em uma decisão que gerou debates, reconheceu a licitude do espelhamento de WhatsApp quando configurado como técnica especial de investigação (infiltração virtual), desde que amparada por autorização judicial e requisitos rigorosos. Essa decisão, embora ainda gere divergências com a 6ª Turma, demonstra uma adaptação judicial à realidade tecnológica, exigindo, em contrapartida, um controle ainda mais rigoroso da cadeia de custódia para evitar violações garantistas.

Infiltração Virtual: A infiltração virtual, regulamentada pela Lei nº 13.441/2017, permite que agentes policiais se infiltrem em redes sociais e aplicativos para coletar provas. O STJ tem exigido autorização judicial prévia e fundamentada, além da observância de um prazo determinado, para que essa técnica seja considerada lícita. A prova obtida por infiltração virtual deve, igualmente, respeitar a cadeia de custódia para garantir sua validade.

5.3 Reconhecimento Facial e Geolocalização: Limites à Intimidade e Privacidade

O uso de tecnologias de reconhecimento facial e dados de geolocalização pelas autoridades policiais e judiciais tem levantado sérias preocupações quanto à violação de direitos fundamentais, especialmente a intimidade e a privacidade:

Reconhecimento Facial: O STJ, no julgamento do Habeas Corpus 598.886/SC (2020), estabeleceu diretrizes rigorosas para o reconhecimento de pessoas, aplicáveis por analogia ao reconhecimento facial. A decisão exige que o procedimento seja realizado em conformidade com o art. 226 do CPP, sob pena de nulidade. A utilização de bancos de dados de reconhecimento facial sem critérios claros, sem autorização judicial e sem a garantia de que os dados foram coletados licitamente, tem sido questionada. A perspectiva garantista exige que o uso dessa tecnologia seja proporcional, subsidiário e sempre sob controle judicial, para evitar a criação de um Estado de vigilância em massa.

Dados de Geolocalização: O acesso a dados de geolocalização, que revelam o paradeiro de um indivíduo, é uma medida invasiva que atinge diretamente a privacidade. O Supremo Tribunal Federal (STF), embora não tenha um precedente específico sobre geolocalização no processo penal, tem se posicionado pela necessidade de autorização judicial para a quebra de sigilo de dados, por analogia à quebra de sigilo telefônico e de dados telemáticos (ADPF 347). A obtenção de dados de geolocalização sem ordem judicial ou fora dos parâmetros legais configura prova ilícita, sujeita à teoria dos frutos da árvore envenenada.

5.4 A Relativização da Cadeia de Custódia em Casos Específicos: Análise Crítica

Embora a jurisprudência majoritária dos tribunais superiores reforce a importância da cadeia de custódia, tem-se observado, em alguns julgados, uma tendência à sua relativização em casos específicos, especialmente quando a quebra não gera prejuízo

concreto à defesa ou quando a prova é corroborada por outros elementos. Essa relativização, contudo, deve ser vista com cautela.

Em novembro de 2025, o STJ, em um caso envolvendo violência doméstica, admitiu *prints* de WhatsApp obtidos por particulares, mesmo com falhas na cadeia de custódia, argumentando que a quebra não implicaria nulidade automática, mas transferiria o ônus de demonstrar o prejuízo ou a manipulação para a parte interessada. Embora a intenção seja proteger vítimas vulneráveis, essa abordagem pode abrir precedentes perigosos, fragilizando a exigência de integridade da prova e o *standard* de prova da acusação.

A quebra da cadeia de custódia é, por si só, um prejuízo à confiabilidade da prova. Exigir que a defesa prove a manipulação é inverter o ônus e desconsiderar a dificuldade técnica de tal comprovação. A presunção de inocência e o *in dubio pro reo* demandam que a prova seja apresentada pelo Estado com sua integridade garantida. A relativização da cadeia de custódia, mesmo em casos de boa-fé, pode minar a racionalidade do processo penal e abrir portas para a arbitrariedade, transformando a cadeia de custódia em um mero formalismo esvaziado de conteúdo. A integridade da prova digital é um direito fundamental do acusado, e sua violação deve, em regra, levar à sua inadmissibilidade.

6. CONCLUSÃO

A era digital, com sua onipresença e constante evolução, impôs ao Direito Processual Penal desafios sem precedentes, especialmente no que tange à produção e valoração da prova. O presente texto buscou demonstrar que a cadeia de custódia digital não é um mero detalhe técnico ou uma formalidade burocrática, mas um pilar fundamental do garantismo penal na contemporaneidade, essencial para assegurar a validade, a confiabilidade e a legitimidade das evidências eletrônicas.

Partindo dos fundamentos do garantismo de Luigi Ferrajoli, que preconiza a limitação do poder punitivo estatal e a proteção das liberdades individuais através de um rigoroso sistema de garantias, evidenciou-se que a verdade processual é uma verdade aproximada e controlável, construída dialeticamente sob o crivo do contraditório e da ampla defesa. Nesse contexto, a prova ilícita, obtida em violação a direitos fundamentais, e suas derivadas, são inadmissíveis, atuando como um freio ético e jurídico à arbitrariedade.

A análise da prova digital revelou suas características intrínsecas de volatilidade, mutabilidade e fragilidade, que a distinguem das provas materiais tradicionais e exigem *standards* técnicos rigorosos, como os preconizados pela ISO/IEC 27037. O advento da prova em nuvem e da criptografia de ponta a ponta adiciona camadas de complexidade, demandando novas abordagens e um constante equilíbrio entre a eficácia investigativa e a proteção da privacidade.

A positivação da cadeia de custódia no Código de Processo Penal pelo Pacote Anticrime (Lei nº 13.964/2019) representou um avanço legislativo crucial. As etapas detalhadas da cadeia de custódia do reconhecimento ao descarte são mecanismos que visam a garantir a integridade do vestígio digital. A quebra da cadeia de custódia, nesse sentido, não é uma falha menor, mas uma violação que compromete a confiabilidade da prova e, sob uma

ótica garantista, deve levar à sua nulidade, independentemente da demonstração de prejuízo concreto, pois o prejuízo é inerente à perda da presunção de integridade.

A jurisprudência dos Tribunais Superiores, especialmente do STJ e STF entre 2020 e 2025, tem sido um termômetro da evolução e dos desafios enfrentados. O precedente da "Operação Open Doors" (RHC 143.169/RJ) consolidou a importância da cadeia de custódia para a validade de mensagens de WhatsApp. As decisões mais recentes sobre espelhamento de WhatsApp, *prints* e o acesso da defesa às mídias originais reforçam a necessidade de um controle rigoroso. Contudo, a tendência de relativização da cadeia de custódia em alguns casos, embora com boas intenções, deve ser vista com cautela, pois pode fragilizar o sistema de garantias e inverter o ônus da prova.

Em suma, a cadeia de custódia digital é a materialização do garantismo penal na era tecnológica. Ela é a ponte entre a busca pela verdade e o respeito aos direitos fundamentais. Para um processo penal justo e democrático, é imperativo que todos os operadores do direito, policiais, peritos, promotores, advogados e juízes, compreendam e apliquem rigorosamente os preceitos da cadeia de custódia. Somente assim será possível construir uma verdade processual sólida, transparente e que não se curve aos atalhos da arbitrariedade, garantindo que a justiça seja feita com base em provas íntegras e confiáveis.

7. REFERÊNCIAS BIBLIOGRÁFICAS

[1] FERRAJOLI, Luigi. *Diritto e Ragione: Teoria del garantismo penale*. Roma-Bari: Laterza, 1989

[2] JUSBRASIL.*A Cadeia de Custódia Digital como Expressão do Garantismo Jurídico*. Disponível em: https://www.jusbrasil.com.br/artigos/a-cadeia-de-custodia-digital-como-expressao-do-garantismo-juridico-entre-o-controle-do-poder-punitivo-e-a-racionalidade-da-prova-no-processo-penal-brasileiro/5285856303. Acesso em: 27 nov. 2025

[3] FERRAJOLI, Luigi.*Op. cit.*, p. 45

[4] TARUFFO, Michele.*La prova dei fatti giuridici*. Milano: Giuffrè, 1992

[5] BADARÓ, Gustavo Henrique.*Processo Penal*. São Paulo: Thomson Reuters Brasil, 2023

[6] PRADO, Geraldo.*A Cadeia de Custódia da Prova no Processo Penal*. São Paulo: Marcial Pons, 2019

[7] CONJUR.*Prova digital foi em 2025 e será em 2026 o grande tema do processo penal*. Disponível em: https://www.conjur.com.br/2025-dez-26/prova-digital-foi-em-2025-e-sera-em-2026-o-grande-tema-do-processo-penal/. Acesso em: 30 nov. 2025

[8] JUSBRASIL.*A Cadeia de Custódia Digital como Expressão do Garantismo Jurídico*. Disponível em: https://www.jusbrasil.com.br/artigos/a-cadeia-de-custodia-digital-como-expressao-do-garantismo-juridico-entre-o-controle-do-poder-punitivo-e-a-racionalidade-da-prova-no-processo-penal-brasileiro/5285856303. Acesso em: 01 dez. 2025

[9] MIGALHAS.*Uso de prova de prints de WhatsApp à luz da jurisprudência do STJ*. Disponível em: https://www.migalhas.com.br/coluna/migalhas-criminais/445874/uso-de-prova-de-prints-de-whatsapp-a-luz-da-jurisprudencia-do-stj. Acesso em: 01 dez. 2025

[10] ISO/IEC 27037:2012.*Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. Disponível em: https://www.iso.org/standard/52817.html. Acesso em: 05 dez. 2025

[11] CNJ.*Necessidade de padronização pelo Conselho Nacional de Justiça da cadeia de custódia da prova digital*. Disponível em: https://www.conjur.com.br/2025-jul-23/necessidade-de-padronizacao-pelo-conselho-nacional-de-justica-da-cadeia-de-custodia-da-prova-digital/. Acesso em: 10 dez. 2025

[12] MIGALHAS.*iPhones sem portas: O desafio da perícia em um mundo 100% em nuvem*. Disponível em: https://www.migalhas.com.br/depeso/434929/iphones-sem-portas-o-desafio-da-pericia-em-um-mundo-100-em-nuvem. Acesso em: 20 dez. 2025

[13] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 dez. 2025

[14] BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), e a Lei nº 7.210, de 11 de julho de 1984 (Lei de Execução Penal), para aprimorar a legislação penal e processual penal. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 24 dez. 2025

[15] STJ. AgRg no RHC 143.169/RJ. Relator: Ministro Ribeiro Dantas. Julgado em 09/03/2021. Disponível em:https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2021/09032021-STJ-anula-provas-digitais-por-falta-de-cadeia-de-custodia.aspx. Acesso em: 01 jan. 2026

[16] JUSBRASIL.*A Cadeia de Custódia Digital como Expressão do Garantismo Jurídico*. Disponível em: https://www.jusbrasil.com.br/artigos/a-cadeia-de-custodia-digital-como-expressao-do-garantismo-juridico-entre-o-controle-do-poder-punitivo-e-a-racionalidade-da-prova-no-processo-penal-brasileiro/5285856303. Acesso em: 01 jan. 2026

[17] CONJUR.*Necessidade de padronização pelo Conselho Nacional de Justiça da cadeia de custódia da prova digital*. Disponível em: https://www.conjur.com.br/2025-jul-23/necessidade-de-padronizacao-pelo-conselho-nacional-de-justica-da-cadeia-de-custodia-da-prova-digital/. Acesso em: 02 jan. 2026

[18] STJ. AgRg no RHC 143.169/RJ. Relator: Ministro Ribeiro Dantas. Julgado em 09/03/2021. Disponível em:https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2021/09032021-STJ-anula-provas-digitais-por-falta-de-cadeia-de-custodia.aspx. Acesso em: 03 jan. 2026

[19] MIGALHAS.*Uso de prova de prints de WhatsApp à luz da jurisprudência do STJ*. Disponível em: https://www.migalhas.com.br/coluna/migalhas-criminais/445874/uso-de-prova-de-prints-de-whatsapp-a-luz-da-jurisprudencia-do-stj. Acesso em: 07 jan. 2026

[20] ESTRATEGIA CONCURSOS.*Prints de WhatsApp em violência doméstica: cadeia de custódia*. Disponível em: https://cj.estrategia.com/portal/prints-whatsapp-violencia-domestica-cadeia-custodia/. Acesso em: 07 jan. 2026

[21] CONJUR.*(In)admissibilidade probatória do espelhamento do WhatsApp: dos critérios jurisprudenciais*. Disponível em: https://www.conjur.com.br/2025-nov-01/inadmissibilidade-probatoria-do-espelhamento-do-whatsapp-analise-critica-dos-criterios-jurisprudenciais-e-proposta-de-standards-de-controle/. Acesso em: 07 jan. 2026

[22] BRASIL. Lei nº 13.441, de 8 de maio de 2017. Altera a Lei nº 12.850, de 2 de agosto de 2013, para dispor sobre a infiltração de agentes de polícia na internet. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13441.htm. Acesso em: 07 jan. 2026

[23] STJ. Habeas Corpus nº 598.886/SC. Relator: Ministro Rogério Schietti Cruz. Julgado em 27/10/2020. Disponível em:https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2020/27102020-Quinta-Turma-do-STJ-estabelece-novas-regras-para-o-reconhecimento-de-pessoas.aspx. Acesso em: 07 jan. 2026

[24] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em:http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 jan. 2026.