

Integridade e rastreabilidade da prova digital em apurações de assédio moral no trabalho.

Integrity and traceability of digital evidence in workplace moral harassment investigations.

Roberson Paulo da Silva

RESUMO

A incorporação de ferramentas digitais ao cotidiano profissional modificou a maneira pela qual fatos ocorridos no trabalho podem ser registrados, preservados e posteriormente avaliados. Em apurações de assédio moral, mensagens eletrônicas, correios corporativos, registros de sistemas, arquivos de áudio, imagens e documentos digitais podem contribuir para reconstruir episódios que, muitas vezes, não foram presenciados por terceiros. A existência de um registro, entretanto, não resolve por si só o problema probatório. É necessário conhecer sua origem, as condições em que foi obtido, as operações realizadas sobre ele, os responsáveis por seu manuseio e as circunstâncias de sua apresentação. Este artigo analisa a cadeia de custódia como instrumento de rastreabilidade da prova digital em investigações de assédio moral no trabalho. A pesquisa adota abordagem qualitativa, bibliográfica e documental, tomando como base o material acadêmico fornecido e a estrutura conceitual nele desenvolvida. Examina-se a relação entre prova digital, proteção de dados, privacidade, autenticidade, integridade e contexto. Também são discutidos o hash criptográfico e a blockchain, destacando-se suas utilidades e limitações. Sustenta-se que nenhuma ferramenta tecnológica, isoladamente, assegura a veracidade do conteúdo ou a licitude da obtenção. A confiabilidade decorre de um procedimento integrado,

capaz de documentar a trajetória do dado desde sua identificação até sua apresentação. Ao final, propõe-se um fluxo operacional proporcional, destinado a reduzir perdas, alterações, seleções indevidas e dúvidas sobre a origem dos registros.

Palavras-chave: prova digital; cadeia de custódia; assédio moral; investigação interna; proteção de dados; rastreabilidade.

ABSTRACT

The incorporation of digital tools into everyday professional life has changed the ways in which workplace events may be recorded, preserved and assessed. In moral-harassment investigations, electronic messages, corporate emails, system records, audio files, images and digital documents may help reconstruct events that were not directly witnessed by third parties. The existence of a digital record, however, does not by itself resolve the evidentiary problem. Its source, acquisition conditions, subsequent operations, handlers and presentation circumstances must also be understood. This article examines chain of custody as a mechanism for tracing digital evidence in workplace moral-harassment investigations. It adopts a qualitative, bibliographic and documentary approach, based on the academic material supplied and on the conceptual framework developed therein. The analysis addresses the relationship among digital evidence, data protection, privacy, authenticity, integrity and context. Cryptographic hashing and blockchain are also discussed, with emphasis on their practical uses and limitations. The central argument is that no technological tool, standing alone, guarantees the truthfulness of content or the legality of its acquisition. Reliability depends on an integrated procedure capable of documenting the path of data from identification to presentation. Finally, a proportional operational flow is proposed to reduce loss, alteration, improper selection and uncertainty concerning the origin of digital records.

Keywords: digital evidence; chain of custody; workplace harassment; internal investigation; data protection; traceability.

1 INTRODUÇÃO

A presença de tecnologias digitais nas relações de trabalho produziu uma alteração profunda na forma como as atividades profissionais são realizadas e documentadas. Comunicação

por correio eletrônico, plataformas corporativas, aplicativos de mensagens, sistemas de gestão e ambientes compartilhados tornou-se parte ordinária da vida organizacional. Como consequência, acontecimentos relevantes para uma investigação podem deixar rastros eletrônicos mesmo quando não existe documentação física ou testemunho direto de todos os episódios.

Essa nova realidade amplia as possibilidades de demonstração dos fatos, mas também introduz problemas que não aparecem com a mesma intensidade na prova tradicional. Um documento digital pode ser duplicado sem perda perceptível, armazenado em diferentes ambientes, sincronizado entre dispositivos e submetido a operações que alteram seu conteúdo ou seus metadados. A facilidade de reprodução, portanto, não equivale a confiabilidade.

A dificuldade é particularmente expressiva em situações de assédio moral. Condutas abusivas podem desenvolver-se de maneira progressiva, em diferentes momentos e canais, dentro de relações marcadas por desigualdade hierárquica. Uma mensagem isolada pode ter significado limitado; a mesma mensagem, integrada a uma sucessão de cobranças, exclusões, alterações de tarefas ou comentários depreciativos, pode adquirir relevância distinta. A prova precisa ser lida em conjunto e em ordem temporal.

Nesse cenário, surge o problema central do estudo: como organizar a prova digital de modo que sua trajetória possa ser conhecida e criticada, sem ampliar a investigação para além do necessário e sem violar a privacidade das pessoas envolvidas? A resposta exige aproximação entre técnica de preservação, normas jurídicas e critérios de investigação.

O objetivo geral é analisar a cadeia de custódia como mecanismo de rastreabilidade da prova digital em apurações de assédio moral no trabalho. Busca-se, especificamente, compreender as características da prova digital; diferenciar autenticidade, integridade, contexto e procedência; examinar a utilidade metodológica da cadeia de custódia; discutir os limites da coleta empresarial; avaliar o papel do hash e da blockchain; e apresentar um procedimento operacional proporcional.

A hipótese é que a qualidade da prova depende menos da sofisticação isolada da tecnologia do que da coerência do processo de preservação. Registros produzidos contemporaneamente aos atos, identificação dos responsáveis, controle de acesso, documentação das decisões e explicitação das limitações aumentam a possibilidade de uma avaliação crítica posterior.

O trabalho adota método qualitativo, bibliográfico e documental. A organização temática parte do material acadêmico fornecido, que apresenta a cadeia de custódia como eixo de confiabilidade da prova digital e destaca a necessidade de conciliar investigação, privacidade e proteção de dados. □ filecite□turn0file0□ L82-L109 A presente redação foi integralmente reconstruída, com formulação própria, ampliação das relações argumentativas e reorganização dos parágrafos, preservando apenas as ideias e referências necessárias ao desenvolvimento do tema.

2 ASSÉDIO MORAL E A TRANSFORMAÇÃO DIGITAL DO CONJUNTO PROBATÓRIO

O estudo da prova digital em casos de assédio moral não pode começar pelo arquivo isoladamente considerado. É necessário compreender que a ocorrência do comportamento abusivo está relacionada a circunstâncias concretas: posição hierárquica, repetição de condutas quando pertinente, ambiente de trabalho, conteúdo das comunicações e consequências produzidas. O registro eletrônico é uma peça de um conjunto mais amplo.

A digitalização alterou também o espaço em que os conflitos se manifestam. Uma cobrança pode ser encaminhada fora do estabelecimento físico; uma reprimenda pode aparecer em grupo corporativo; a retirada de determinado trabalhador de uma ferramenta de comunicação pode ficar registrada no sistema. O ambiente virtual, nesses casos, não é exterior à relação de trabalho, mas uma de suas formas contemporâneas de manifestação.

O fator temporal ganha especial importância. A análise de mensagens em ordem cronológica pode revelar repetição, escalada ou mudança de comportamento que não seria percebida na leitura fragmentada. Por essa razão, o investigador deve preservar, sempre que pertinente, elementos anteriores e posteriores ao trecho que inicialmente motivou a apuração.

Essa preocupação leva à distinção entre conteúdo e evidência. Conteúdo é o que aparece no arquivo; evidência é o significado que esse conteúdo assume diante de uma hipótese factual. Uma imagem de tela pode reproduzir uma frase com precisão e, ainda assim, não indicar se a conversa estava completa, de onde veio, quem efetuou a captura ou se outros elementos alterariam sua interpretação.

O material fornecido destaca justamente os riscos de edição, supressão e perda de contexto e relaciona a qualidade da documentação ao potencial de influência do artefato sobre

uma decisão. filecite turn0file0 L141-L160 Em outras palavras, quanto maior o impacto esperado da prova, maior deve ser a preocupação com sua história.

Também existe o risco de confirmação da hipótese inicial. Uma investigação pode ser iniciada após relato de assédio e, inadvertidamente, tornar-se uma busca por elementos que confirmem o relato. O procedimento adequado deve manter abertura para informações favoráveis e desfavoráveis à hipótese. A imparcialidade não significa ausência de conclusão, mas compromisso com um processo que permita que os dados contrariem a expectativa inicial.

Assim, a cadeia de custódia não deve ser tratada como técnica para provar o assédio. Ela cumpre função anterior e diferente: permitir que se saiba de onde veio o dado, como foi tratado e em que medida a representação apresentada corresponde ao material que existia no momento da preservação.

3 FUNDAMENTOS JURÍDICOS E LIMITES DA PRESERVAÇÃO

A cadeia de custódia recebeu disciplina expressa no Código de Processo Penal com a introdução dos arts. 158-A a 158-F pela Lei n. 13.964/2019. O modelo legal procura registrar a história cronológica do vestígio e suas etapas de reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, processamento, armazenamento e descarte. No entanto, a literalidade dessas normas está vinculada ao processo penal.

Por essa razão, em investigações trabalhistas privadas, a cadeia de custódia deve ser empregada como referência metodológica, e não como reprodução automática do procedimento penal. A finalidade é aproveitar os conceitos de rastreabilidade e documentação sem ignorar a natureza específica da relação laboral e os direitos das pessoas envolvidas.

O Código de Processo Civil oferece outro ponto de apoio ao estabelecer a utilização de meios legais e moralmente legítimos para demonstração dos fatos e atribuir ao julgador a tarefa de apreciar a prova constante dos autos. Isso evidencia que a discussão não se reduz à existência material de um arquivo: importa saber como ele foi produzido, preservado e relacionado aos demais elementos.

Também é necessário distinguir quatro planos. A licitude refere-se às condições jurídicas da obtenção. A autenticidade diz respeito à correspondência entre o elemento apresentado e a origem que lhe é atribuída. A integridade relaciona-se à manutenção do objeto entre estados

comparados. O contexto diz respeito à relação do registro com a sequência factual. A cadeia de custódia contribui para conectar esses planos, mas não os substitui.

Os direitos fundamentais estabelecem limites ainda mais importantes. Intimidade, vida privada, honra, imagem e sigilo de comunicações e dados não desaparecem porque a investigação ocorre dentro de uma empresa. A existência de infraestrutura corporativa não autoriza acesso ilimitado a todo conteúdo que possa ser tecnicamente alcançado.

A proteção de dados acrescenta princípios de finalidade, adequação, necessidade, segurança, prevenção, transparência e responsabilização. O material original enfatiza que a coleta deve ser suficiente para esclarecer a hipótese, sem transformar preservação em justificativa para guardar indiscriminadamente tudo o que estiver disponível. filecite turn0file0 □L198-L212

□ A consequência prática é a necessidade de delimitação prévia. Deve-se definir o objetivo da investigação, o período relevante, as fontes que poderão ser acessadas, as pessoas autorizadas, os critérios de pertinência e o período de retenção. A proteção jurídica não impede uma apuração legítima; exige que ela seja justificável.

4 A CADEIA DE CUSTÓDIA COMO HISTÓRIA DO DADO

A melhor maneira de compreender a cadeia de custódia no ambiente digital é tratá-la como uma história documentada do objeto probatório. Essa história deve permitir responder perguntas simples: quando o elemento foi identificado? Quem o preservou? Qual era sua condição? Qual ferramenta foi utilizada? Houve cópia? Quem acessou? O arquivo foi transformado? Qual versão foi apresentada?

O primeiro passo é a identificação das fontes. A equipe deve mapear, de acordo com a hipótese, quais sistemas podem conter informação relevante. Essa decisão precisa ser fundamentada, porque o acesso a uma fonte digital não deve ser consequência apenas de sua disponibilidade técnica.

Em seguida vem a preservação. Seu propósito é evitar que o dado desapareça ou seja alterado por funcionamento normal do sistema. Mensagens podem ser excluídas por políticas de retenção, logs podem ser sobrescritos e contas podem mudar de configuração. A providência adequada depende da arquitetura da fonte.

A documentação acompanha a preservação. O registro deve individualizar o item, sua origem, a data e o horário, o responsável, a ferramenta utilizada, o procedimento realizado e o local de armazenamento. A finalidade é permitir auditoria posterior e reduzir a dependência da memória dos investigadores.

Na aquisição, deve-se preferir método que preserve o máximo possível das características relevantes da fonte. A distinção entre fonte preservada, cópia de trabalho e produto analítico é essencial. O analista pode filtrar, classificar e destacar informações em sua cópia de trabalho, mas essas alterações não devem ser confundidas com modificações do material preservado.

O armazenamento também integra a cadeia. O acesso deve ser restrito, registrado e compatível com a finalidade. Cópias adicionais podem existir, desde que sua relação com a fonte esteja documentada. A multiplicidade de cópias, em si, não rompe a rastreabilidade; o problema surge quando não se sabe qual versão corresponde a qual etapa.

O material de referência ressalta que não basta registrar o que foi preservado. Também é importante documentar aquilo que não foi obtido e explicar a razão da ausência.

filecite □turn0file0□L250-L258□ Essa transparência é especialmente valiosa quando a investigação utiliza apenas determinados canais ou intervalos temporais.

5 PROCEDIMENTOS DE COLETA E PRESERVAÇÃO

Uma investigação organizada começa com uma matriz de apuração. Nela podem constar a hipótese provisória, o período investigado, as pessoas ou unidades relacionadas, as fontes autorizadas, os responsáveis e os critérios para encerramento. Essa etapa reduz o risco de a investigação crescer indefinidamente em busca de qualquer informação potencialmente útil.

A preservação deve considerar o ciclo de vida do sistema. Um servidor pode conservar registros por determinado período; um aplicativo pode permitir exportação limitada; um serviço em nuvem pode disponibilizar mecanismos específicos de retenção. O investigador precisa conhecer essas características para decidir quais medidas são possíveis.

A cronologia merece tratamento próprio. Sistemas distintos podem utilizar fusos, formatos ou referências temporais diferentes. O horário mostrado na tela pode não ser idêntico ao horário registrado no servidor. A diferença deve ser explicada tecnicamente antes de ser interpretada como indício de alteração.

Outro ponto é a identificação dos profissionais. Investigador, técnico de aquisição e analista devem ser individualizados. Quando uma mesma pessoa exerce mais de uma função, isso deve aparecer na documentação. A segregação de funções, quando viável, reduz o risco de alterações não detectadas e melhora a capacidade de revisão.

As ferramentas empregadas também precisam ser registradas. Versões diferentes de programas podem processar determinados dados de maneiras diferentes. Informar o software e sua versão permite compreender o método utilizado e, quando necessário, repetir a operação.

A proteção de dados acompanha todo o procedimento. Deve-se limitar o número de pessoas com acesso, proteger o armazenamento, controlar compartilhamentos e definir critérios de descarte. O material de origem ressalta que segurança e prevenção devem integrar todas as fases da investigação.

Finalmente, é necessário registrar os critérios de seleção. Se apenas determinado conjunto de mensagens foi preservado, deve-se indicar por quê. Essa explicação não obriga a empresa a armazenar toda a comunicação de seus empregados; apenas permite que posteriormente se avalie a razoabilidade do recorte.

6 HASH E VERIFICAÇÃO DA INTEGRIDADE

O hash criptográfico ocupa posição relevante na preservação digital porque permite comparar o estado de um arquivo em momentos diferentes. Ao calcular um valor sobre determinado objeto no momento da preservação e repetir o cálculo posteriormente, é possível verificar se as entradas comparadas permanecem correspondentes.

Esse mecanismo, entretanto, não deve receber função maior do que aquela que efetivamente possui. O hash não informa se o arquivo inicial era completo, verdadeiro, licitamente obtido ou corretamente selecionado. Ele apenas permite detectar alteração entre estados comparados.

O exemplo da conversa eletrônica evidencia o problema. Se alguém seleciona um trecho, elimina o restante e calcula o hash depois, o resultado será tecnicamente consistente. O algoritmo não tem como saber que havia mensagens ausentes. A integridade da cópia não equivale à integridade do contexto.

Por isso, o valor do hash depende da qualidade da etapa anterior. Origem, método de aquisição, responsável, momento da coleta e relação entre o objeto original e suas cópias

precisam estar documentados. Se houver conversão de formato, transcrição ou outra transformação legítima, o resultado deve ser identificado como derivado.

O próprio material de referência ressalta que a função criptográfica não alcança os acontecimentos anteriores à sua aplicação. □ filecite turn0file0 □ L314-L355 Essa observação impede que o hash seja apresentado como certificado absoluto de autenticidade.

A autenticidade pode ser reforçada por informações independentes: registros de servidor, metadados, cabeçalhos de e-mail, autenticação, documentos correlatos e testemunhos. A convergência desses elementos pode produzir quadro probatório mais sólido do que a confiança exclusiva em um mecanismo criptográfico.

A distinção é fundamental para evitar tecnicismo vazio. A tecnologia deve servir à explicação da prova. Quando o procedimento consegue demonstrar como o arquivo chegou ao estado preservado, o hash acrescenta uma verificação objetiva. Quando a origem é desconhecida, o hash apenas documenta a versão que foi encontrada.

7 BLOCKCHAIN E A CONSTRUÇÃO DE CONFIANÇA

A blockchain pode funcionar como camada adicional de registro de eventos de custódia. Sua utilidade, nesse contexto, está menos no armazenamento do conteúdo e mais na possibilidade de ancorar informações que permitam verificar posteriormente a existência de determinado estado do objeto.

Uma arquitetura prudente mantém o conteúdo sensível em repositório protegido e registra externamente apenas o mínimo necessário, como resumo criptográfico e informações temporais. Essa separação reduz a exposição de dados pessoais e evita transformar a infraestrutura de registro em depósito permanente de informações potencialmente sensíveis.

A vantagem, porém, não é absoluta. Se o arquivo foi adulterado antes de sua ancoragem, a blockchain registrará a versão adulterada. A tecnologia pode dificultar a alteração posterior do registro, mas não corrige a entrada defeituosa.

A governança também é relevante. É necessário saber quem administra a rede, quem pode registrar eventos, quais regras orientam a validação e como os acessos são controlados. A palavra 'imutável' não deve ser empregada sem explicar o sistema concreto a que se refere.

O material original apresenta a blockchain como possibilidade adicional, não como condição de validade da prova. □ filecite turn0file0 □ L363-L408 Essa posição é

metodologicamente mais segura. Em casos simples, um sistema de logs protegido e auditável pode atender ao objetivo com menor custo e complexidade.

A escolha da ferramenta deve acompanhar o risco. Casos de grande volume, elevado potencial de litígio ou necessidade de auditoria independente podem justificar mecanismos mais sofisticados. Em investigações menores, a tecnologia mais simples pode ser suficiente se produzir registros confiáveis e protegidos.

8 INVESTIGAÇÃO INTERNA, PRIVACIDADE E GOVERNANÇA

A investigação privada apresenta característica que não pode ser ignorada: a organização que coleta a prova geralmente possui interesse direto ou indireto no resultado. Ao mesmo tempo, possui capacidade técnica de acessar grande quantidade de informações. Essa combinação torna a governança particularmente importante.

A distribuição de responsabilidades é uma primeira salvaguarda. Quem recebe a denúncia não precisa ser a mesma pessoa que extrai os dados, e quem analisa tecnicamente não deve necessariamente ser quem decide a consequência disciplinar. A separação possível entre funções reduz conflitos e melhora a supervisão.

A finalidade constitui a segunda salvaguarda. A existência de acesso administrativo a um sistema não significa que qualquer informação possa ser utilizada para qualquer objetivo. A fonte precisa ser pertinente e o período escolhido deve possuir relação com a hipótese.

A segurança constitui a terceira camada. Dados de investigação podem conter informações pessoais, relatos sensíveis, comunicações de terceiros e informações estratégicas. Controle de acesso, autenticação, armazenamento protegido e registro das operações são medidas que reduzem riscos.

A imparcialidade é igualmente necessária. Uma investigação que conserva apenas elementos acusatórios pode produzir uma narrativa artificialmente completa. Elementos que contrariem a hipótese devem ser tratados com o mesmo cuidado.

Também é indispensável registrar limitações. Uma plataforma pode não permitir exportação integral; um período pode já ter sido perdido; um equipamento pode não estar disponível. A ausência desses dados deve ser explicitada para evitar que o relatório transmita falsa impressão de completude.

A retenção precisa ser proporcional. O encerramento da investigação não transforma todos os dados coletados em material que deve permanecer armazenado indefinidamente. O descarte, quando juridicamente possível, também deve ser documentado.

O material fornecido enfatiza que privacidade não é obstáculo externo à investigação, mas condição de legitimidade do procedimento. Uma prova obtida de modo ilícito não se torna legítima porque posteriormente foi protegida por hash ou blockchain.

9 VALORAÇÃO DA PROVA E CONTRADITÓRIO

A finalidade prática da cadeia de custódia aparece com maior clareza quando a prova é submetida à apreciação. Nesse momento, não basta mostrar o conteúdo. É necessário possibilitar que se examine sua origem, integridade, contexto e percurso.

Um print de tela, por exemplo, não deve ser classificado automaticamente como inútil. Sua força dependerá da possibilidade de relacioná-lo à fonte, à pessoa que o produziu, ao dispositivo, ao contexto da conversa e a outros elementos. A análise deve ser concreta.

Quando a cadeia está documentada, uma discussão sobre eventual adulteração pode ser deslocada para pontos verificáveis. Podem ser examinados o hash, o método de aquisição, os registros de acesso, a ferramenta empregada e as versões existentes. Sem documentação, a controvérsia tende a se limitar a afirmações incompatíveis.

O contraditório não exige exposição irrestrita de todos os dados. Informações de terceiros ou elementos sem pertinência podem exigir proteção. Cópias controladas, ocultação de dados irrelevantes e acesso supervisionado são alternativas que podem equilibrar transparência e privacidade.

Também não se deve confundir falha de custódia com nulidade automática de qualquer elemento. A consequência de uma irregularidade deve levar em conta sua gravidade, o impacto sobre a confiabilidade, a possibilidade de verificação posterior e a existência de outros elementos convergentes.

A cadeia de custódia aumenta a qualidade do debate justamente porque torna o dado questionável de maneira racional. Quanto melhor documentado o caminho percorrido, mais específico pode ser o questionamento sobre sua autenticidade e significado. O documento de origem destaca essa função de qualificação do debate probatório.

10 PROPOSTA DE PROCEDIMENTO PARA APURAÇÕES DE ASSÉDIO MORAL

A partir das premissas anteriores, pode-se organizar a investigação em oito fases articuladas. O objetivo não é impor um modelo único a todas as organizações, mas oferecer uma referência mínima que possa ser adaptada ao tamanho da investigação, à sensibilidade dos dados e à arquitetura tecnológica.

10.1 Abertura e delimitação

A denúncia deve ser identificada e registrada. Devem constar o fato comunicado, período aproximado, pessoas envolvidas, canais relevantes, finalidade e hipótese inicial. Essa hipótese deve permanecer aberta à revisão.

10.2 Preservação

Fontes sujeitas a perda devem receber medidas de retenção compatíveis com seu funcionamento. A decisão deve indicar o que foi preservado, quando, por quem e com qual fundamento. Impossibilidades técnicas também precisam ser registradas.

10.3 Aquisição

A extração deve ser adequada à fonte e, quando possível, preservar o formato nativo e os metadados relevantes. Cópias técnicas devem ser separadas das cópias utilizadas para análise.

10.4 Identificação e integridade

Cada item deve receber identificador próprio. O hash pode ser empregado para verificar a correspondência entre a fonte preservada e suas cópias. Transformações devem ser registradas como derivações.

10.5 Custódia e acesso

O armazenamento deve utilizar controles de acesso e mecanismos de segurança. Cada operação relevante deve ser registrada com identificação do usuário, momento e finalidade.

10.6 Análise

A análise deve ocorrer sobre cópia de trabalho. Filtros, buscas e critérios de seleção precisam ser documentados. Elementos favoráveis e contrários à hipótese devem ser considerados.

10.7 Validação

Antes da conclusão, deve ocorrer revisão por pessoa qualificada. Devem ser verificadas a coerência temporal, a correspondência entre material e conclusão e, quando aplicável, os valores de hash.

10.8 Apresentação e encerramento

O relatório final deve informar fontes, métodos, limitações e resultados. Se houver utilização judicial, devem ser disponibilizados elementos suficientes ao contraditório, respeitando a proteção de dados. O encerramento e eventual descarte devem ser registrados.

O modelo proposto acompanha a estrutura de oito fases já presente no material original, mas a redação foi reconstruída para enfatizar a finalidade de cada etapa e sua relação com a confiabilidade da prova.

11 METODOLOGIA, LIMITAÇÕES E CONTRIBUIÇÕES

A pesquisa é qualitativa, bibliográfica e documental porque seu objetivo é compreender relações entre categorias jurídicas e técnicas, e não produzir medição estatística da ocorrência de assédio moral. A legislação e as referências indicadas no material de origem constituem a base documental, enquanto a análise busca organizar criticamente os problemas apresentados.

Uma primeira limitação está na inexistência de um procedimento único aplicável, em todos os detalhes, a investigações privadas trabalhistas. Por isso, a cadeia de custódia é tratada como referência metodológica, condicionada à situação concreta.

Outra limitação é tecnológica. Diferentes plataformas armazenam informações de formas distintas. Um protocolo rígido pode falhar justamente porque ignora a arquitetura da fonte. O que deve ser permanente são os princípios de identificação, preservação, documentação, segurança e rastreabilidade.

Há ainda limite epistemológico. Uma cadeia perfeita não transforma registros digitais em reprodução integral da realidade. Uma frase pode possuir ironia, ambiguidade ou significado contextual. O procedimento melhora a confiabilidade do registro, mas não substitui a interpretação.

Quanto à blockchain, seus benefícios dependem da estrutura efetivamente utilizada, da governança e da confiabilidade das informações inseridas. Não é possível converter propriedade técnica em conclusão jurídica automática.

A principal contribuição do estudo está na integração entre prova digital e governança. A organização que estabelece previamente critérios de coleta e preservação reduz disputas futuras e evita que decisões relevantes dependam de arquivos cuja origem seja impossível de explicar. A cadeia de custódia passa, assim, a atuar preventivamente, e não apenas depois que surge o litígio.

O material fornecido reconhece a importância de distinguir fontes, ideias e contribuição autoral. Nesta versão, a redação foi elaborada novamente, sem reproduzir frases ou parágrafos do texto-base. As referências foram mantidas como referências acadêmicas, pois originalidade de redação não elimina a obrigação de reconhecer as fontes das ideias jurídicas e técnicas.

12 CONSIDERAÇÕES FINAIS

A transformação digital do trabalho tornou a prova eletrônica um componente relevante das investigações de assédio moral. A mesma tecnologia que amplia a possibilidade de documentação cria problemas de reprodução, alteração, perda, seleção e interpretação. A resposta adequada não está em presumir que todo registro digital seja confiável nem em rejeitá-lo por sua natureza eletrônica.

A cadeia de custódia oferece uma solução metodológica: registrar a trajetória do dado de forma suficientemente clara para que terceiros possam examiná-la. Identificação, preservação, aquisição, documentação, controle de acesso, análise, validação e apresentação formam uma sequência de cuidados que reduz incertezas.

O estudo também demonstrou que hash e blockchain possuem funções delimitadas. O primeiro é útil para verificar correspondência entre estados de um arquivo; a segunda pode reforçar a cronologia de determinados registros. Nenhum deles substitui coleta adequada, contexto, licitude ou avaliação humana.

A proteção de dados deve acompanhar todas as etapas. A investigação precisa possuir finalidade definida, escopo proporcional, segurança, controle de acesso e justificativa para a retenção. Privacidade e confiabilidade probatória não são objetivos incompatíveis: a boa governança busca preservar o que é necessário e proteger o que não é.

A proposta de oito fases representa a contribuição operacional do trabalho. Seu propósito é oferecer uma estrutura adaptável, capaz de orientar investigações pequenas ou complexas conforme o risco e a sensibilidade do material. A sofisticação tecnológica deve ser consequência da necessidade, e não objetivo autônomo.

Conclui-se, portanto, que a prova digital confiável não é resultado de um arquivo isolado ou de uma ferramenta específica. Ela nasce da combinação entre método, documentação, competência técnica, segurança, contexto e respeito aos direitos fundamentais. A cadeia de custódia deve ser vista como uma arquitetura de confiança: não cria a verdade dos fatos, mas melhora as condições para que a verdade possa ser investigada, contestada e avaliada de forma racional.

REFERÊNCIAS

- ALHARBY, Maher; VAN MOORSEL, Aad. Blockchain-based smart contracts: a systematic mapping study. *Computer Science & Information Technology*, 2017. DOI: 10.48550/arXiv.1710.06372.
- BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República.
- BRASIL. Decreto-Lei n. 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF.
- BRASIL. Lei n. 13.105, de 16 de março de 2015. Código de Processo Civil. Brasília, DF.
- BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF.
- BRASIL. Lei n. 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Brasília, DF.
- LYKIDIS, Ioannis; DROSATOS, George; RANTOS, Konstantinos. The use of Blockchain technology in e-government services. *Computers*, v. 10, n. 12, 2021. DOI: 10.3390/computers10120168.
- NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.
- RAMOS PITTARO NEVES, Elisa. Ensaio sobre a cadeia de custódia e a prova digital. *Revista Científica do CPJM*, v. 4, n. 14, p. 151-159, 2025.

STEFFEN, Catiane. Cadeia de custódia da prova digital no Brasil: o que se precisa, o que se tem e por que pensar em blockchain? Revista da EMERJ, v. 27, p. 1-15, 2025. DOI: 10.70622/2236-8957.2025.643.