Revista ARACÊ
ISSN: 2358-2472

A IMPORTÂNCIA DOS METADADOS PARA COMPROVAÇÃO DA AUTENTICIDADE E INTEGRIDADE DAS PROVAS DIGITAIS

THE IMPORTANCE OF METADATA FOR PROVING THE AUTHENTICITY AND INTEGRITY OF DIGITAL EVIDENCE

LA IMPORTANCIA DE LOS METADATOS PARA PROBAR LA AUTENTICIDAD E INTEGRIDAD DE LA EVIDENCIA DIGITAL

https://doi.org/10.56238/arev7n11-131

Data de submissão: 13/10/2025 **Data de publicação:** 13/11/2025

João Pedro Albino
Livre-docente em Sistemas de Informação
Instituição: Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP)
E-mail: jp.albino@unesp.br
Lattes: http://lattes.cnpq.br/9638407992652406
Orcid: https://orcid.org/0000-0001-5965-1869

Ana Cláudia Pires Ferreira de Lima
Doutoranda no Programa de Mídia e Tecnologia
Instituição: Faculdade de Arquitetura, Artes, Comunicação e Design da UNESP – câmpus de Bauru
E-mail: analima@trt15.jus.br
Lattes: http://lattes.cnpq.br/0293267278473464
Orcid: https://orcid.org/0000-0002-5775-9822

Vanderlei Ferreira de Lima
Mestre em Direito Constitucional
Instituição: Centro Universitário Bauru – ITE
E-mail: vflima@sp.gov.br
Lattes: http://lattes.cnpq.br/6683677486823592
Orcid: https://orcid.org/0009-0008-0742-0143

Daniel Pires Ferreira de Lima
Bacharelando em Direito
Instituição: Centro Universitário de Bauru – Instituição Toledo de Ensino
E-mail: danpflima5@gmail.com
Lattes: http://lattes.cnpq.br/9685305519518212
Orcid: https://orcid.org/0009-0007-5998-3274

RESUMO
Na era digital, a produção de provas em processos administrativos ou judiciais passa a incluir uma vasta gama de registros eletrônicos, desde e-mails, postagens nas mídias sociais, geolocalização e mensagens instantâneas até dados de sistemas de gestão de recursos humanos. A comprovação de fatos registrados eletronicamente requer o conhecimento de alguns termos técnicos para que os profissionais do direito saibam produzir e analisar as provas digitais, observando seus requisitos de validade, a fim de garantir sua autenticidade e integridade, desde sua coleta, armazenamento e apresentação no

Revista ARACÊ
ISSN: 2358-2472

processo judicial eletrônico até seu trânsito em julgado, de forma que não sejam adulteradas e contribuam com a efetivação do direito. O objetivo deste artigo é demonstrar como utilizar a tecnologia para analisar a autenticidade e integridade de uma prova digital que foi impugnada, para tornar mais célere e assertiva a prestação da tutela jurisdicional para garantia dos direitos humanos. Para elaboração deste artigo foi realizada pesquisa em artigos científicos, livros e materiais de cursos e palestras. A análise dos metadados é essencial para verificação da autenticidade e integridade das provas digitais, conferindo-lhes maior confiabilidade.

Palavras-chave: Ciência de Dados. Tecnologia. Metadados. Provas Digitais. Efetividade do Direito.

ABSTRACT

In the digital age, the production of evidence in administrative or judicial proceedings now includes a wide range of electronic records, from emails, social media posts, geolocation, and instant messages to data from human resource management systems. Proving electronically recorded facts requires knowledge of certain technical terms, enabling legal professionals to produce and analyze digital evidence, observing its validity requirements, to ensure its authenticity and integrity, from its collection, storage, and presentation in the electronic judicial process until its final judgment, ensuring that it is not tampered with and contributes to the enforcement of the law. The objective of this article is to demonstrate how to use technology to analyze the authenticity and integrity of contested digital evidence, thereby streamlining and asserting the provision of legal protection to guarantee human rights. This article was prepared using research on scientific articles, books, and course and lecture materials. Metadata analysis is essential for verifying the authenticity and integrity of digital evidence, lending it greater reliability.

Keywords: Data Science. Technology. Metadata. Digital Evidence. Effectiveness of Law.

RESUMEN

En la era digital, la producción de pruebas en procedimientos administrativos o judiciales incluye una amplia gama de registros electrónicos, desde correos electrónicos, publicaciones en redes sociales, geolocalización y mensajes instantáneos hasta datos de sistemas de gestión de recursos humanos. La prueba de hechos registrados electrónicamente requiere el conocimiento de ciertos términos técnicos, lo que permite a los profesionales del derecho producir y analizar pruebas digitales, respetando sus requisitos de validez, para garantizar su autenticidad e integridad, desde su recopilación, almacenamiento y presentación en el proceso judicial electrónico hasta la sentencia firme, garantizando su integridad y contribuyendo a la aplicación de la ley. El objetivo de este artículo es demostrar cómo utilizar la tecnología para analizar la autenticidad e integridad de las pruebas digitales impugnadas, agilizando y reforzando así la protección legal para garantizar los derechos humanos. Este artículo se elaboró a partir de la investigación de artículos científicos, libros y materiales de cursos y conferencias. El análisis de metadatos es esencial para verificar la autenticidad e integridad de las pruebas digitales, otorgándoles mayor fiabilidad.

Palabras clave: Ciencia de Datos. Tecnología. Metadatos. Evidencia Digital. Eficacia del Derecho.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

O registro de dados eletrônicos não é novidade, sendo que há tempos temos muitos registros digitais utilizados como prova em processos judiciais. Verificamos os registros de dados desde a primeira transmissão de pacote de dados feita pela ARPANET – precursora da internet em 1969, até a criação do e-mail em 1972, dos arquivos eletrônicos, arquivos de mídia de áudio e vídeo, dados registrados em memória de computadores, HD, disquetes, CDs, arquivos do word, fotografias digitais, até os registros eletrônicos de ponto que começaram a ser mais utilizados em 1990 e as URLs (*Uniform Resource Locator* – "localizador uniforme de recursos"), criadas como parte do desenvolvimento da World Wide Web por Tim Berners-Lee (Berners-Lee e Masinter, 1994) conhecidas como links ou endereço eletrônico, usadas para localizar recursos na internet.

Desde antes da implantação do Processo Judicial Eletrônico, introduzido pela Lei 11.419 de 2006, as provas digitais são produzidas nos processos judiciais, sendo apresentadas em arquivos de mídia (armazenados em disquetes, CDs, pen drives etc.). Entretanto, somente há pouco tempo é que advogados e juízes têm estudado e analisado os metadados da prova digital, através dos quais é possível verificar sua autenticidade (autoria), integridade (que não houve alteração) e temporalidade (a data e hora em que foi produzida), conferindo maior confiabilidade à prova digital.

O grande diferencial da prova digital é sua reprodutibilidade, ou seja, ela é auditável, assim como ocorre na ciência de dados. Qualquer pessoa que for analisar os metadados da prova digital deve chegar aos mesmos resultados se ela for autêntica e íntegra. Seu caminho pode ser refeito desde o início, observando-se a integridade, autenticidade e cadeia de custódia dos dados coletados e sua análise para tomada de decisão.

Neste artigo analisaremos os conceitos de provas digitais e de metadados, seus exemplos e algumas ferramentas de extração dos metadados de fotografias digitais, vídeos, e-mails, mensagens em aplicativos de mensageria e de outras provas digitais. Abordaremos também a forma de coleta e armazenamento dos dados digitais para que possam ser utilizados como prova em processos administrativos ou judiciais, com a preservação da cadeia de custódia desde sua coleta, armazenamento, apresentação nos autos até a sua análise, ressaltando-se a importância do armazenamento das provas digitais de forma íntegra até o prazo final para interposição de ação rescisória e seu trânsito em julgado.

2 METODOLOGIA

Trata-se de pesquisa aplicada, pois gera produtos e processos com finalidades imediatas utilizando conhecimentos gerados em pesquisa básica com tecnologias existentes. Quanto à abordagem

Revista ARACÊ
ISSN: 2358-2472

a pesquisa é qualitativa, de natureza bibliográfica, caracterizando-se pela análise e interpretação de produção acadêmica e científica já publicada sobre os temas de Prova Digital, Metadados e Ciência de Dados.

A pesquisa adotou uma abordagem predominantemente qualitativa, visto que buscou a análise crítica e a contextualização dos conceitos-chave para demonstrar a aplicação da tecnologia na verificação da autenticidade e integridade das provas digitais.

Para a elaboração deste artigo, a coleta de dados foi realizada através de pesquisa em artigos científicos, livros e materiais de cursos e palestras. Essas fontes serviram para fornecer a base teórica e técnica necessária para compreender os requisitos de validade das provas digitais e a importância da análise dos metadados.

Os procedimentos de pesquisa envolveram a seleção de obras relevantes que abordam o conceito de prova digital, a função dos metadados — como o endereço de IP e a URL — e a forma de coleta e armazenamento de dados digitais para preservação da cadeia de custódia. Também foram analisados exemplos de ferramentas tecnológicas de extração de metadados de diferentes mídias, como fotografias digitais, e-mails e mensagens de aplicativos de mensageria.

A análise foi conduzida através da interpretação e comparação das perspectivas teóricas sobre a comprovação da autenticidade e integridade da prova digital (autoria, integridade e temporalidade), bem como a discussão do arcabouço legal aplicável (como o Código de Processo Civil e o Marco Civil da Internet). O objetivo central da análise foi demonstrar como a utilização da tecnologia, especificamente para análise de metadados, pode tornar mais célere e assertiva a prestação da tutela jurisdicional, garantindo a efetividade dos direitos humanos através da produção e análise de provas digitais confiáveis.

3 PROVA DIGITAL

A prova é um instrumento destinado a formar a convicção do juízo sobre a existência ou não de fatos relevantes para o processo e as circunstâncias em que ocorreram.

Mauro Schiavi nos ensina que o direito à prova constitui garantia fundamental processual e um direito fundamental da cidadania para efetividade do princípio do acesso à justiça e, acima de tudo, o acesso a uma ordem jurídica justa (SCHIAVI, 2021, p. 112).

Revista ARACÊ
ISSN: 2358-2472

3.1 CONCEITO

Segundo Capanema (2023), prova digital é a prova contida em dispositivo informático, referente a fatos ocorridos no meio digital ou físico como por exemplo, as provas contidas em sites, computadores, celulares, pen drive e HDs.

Thamay e Tamer (2020, p. 33), conceituam prova digital como "a demonstração de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo".

O Brasil é um dos países onde as pessoas passam mais tempo conectadas na internet, seja pelo celular ou computador. O brasileiro passa 9h13 por dia na internet, segundo dados do Digital 2024 Global Overview Report, ocupando a segunda posição no ranking mundial, ficando atrás da África do Sul. (CROWDSTRIKE, Threat Hunting Report, 2024, apud METROPOLES, 2024).

Essa transformação digital, com o uso cada vez mais frequente da internet e de dispositivos móveis, acarreta a necessidade cada vez maior de obtenção das provas nos meios digitais, a exemplo de e-mails, mensagens em aplicativos instantâneos de mensageria, postagem de imagem, vídeos e textos em mídias sociais, como Facebook®, Instagram®, Youtube®, X®, e geolocalização dos dispositivos móveis, dentre outras provas.

Essa mudança no comportamento humano revela a importância de os profissionais do direito conhecerem alguns procedimentos de coleta e preservação dos dados digitais para garantir sua integridade e não adulteração, para que possam servir como meio de prova judicial.

3.2 APLICABILIDADE

Como vivemos simultaneamente no mundo analógico e virtual, é natural que as provas judiciais dos fatos registrados eletronicamente, ou seja, nato-digitais, sejam apresentadas na forma digital.

Mensagens ou vídeos de conteúdo difamatório postados nas redes sociais são fatos ocorridos no meio digital e que são objeto de prova em processos com pedido de indenização por danos morais. Uma compra pela internet ou transação bancária online, que já nascem no ambiente digital, são comprovadas através dos respectivos registros digitais.

O meio digital também pode servir de instrumento para comprovar fatos ocorridos em meio não digital. Isso acontece quando fatos do mundo físico são registrados em mídias digitais, como, por exemplo, um vídeo que capta um acidente de trânsito ou fotos digitais retratando momentos da vida de uma pessoa.

Portanto, qualquer documento eletrônico, que dele se extraia um fato jurídico, pode ser utilizado como prova digital.

Revista ARACÊ
ISSN: 2358-2472

A prova digital é uma prova documental. Para Thamay e Tamer (2020, p. 113/114):

> Documento, portanto, é qualquer suporte físico ou eletrônico em que um fato e suas circunstâncias estão registrados. A prova documental, por sua vez, é o resultado obtido no processo ou procedimento a partir da utilização desse documento.
> É prova documental, por exemplo, o resultado prova obtido no processo a partir de CD, mídia ou HD juntado aos autos em que consta determinado vídeo que interessa à discussão jurídica estabelecida. Também é prova documental o resultado no processo a partir da juntada de extratos de registros eletrônicos (IP, data e hora) obtidos em demanda anterior de quebra de sigilo em face de provedor. As capturas de tela ou *printscreen* também produzem provas documentais. Em suma, o fato está registado em algum suporte físico ou eletrônico? E esse suporte não é outra prova específica? Se a resposta for positiva para ambas as questões, o resultado prova extraído será documental.

3.3 LEGISLAÇÃO

Se a prova digital é uma prova documental, todo regramento aplicado às provas documentais, aplicam-se às provas digitais, tanto é que a lei do processo eletrônico assim dispõe em seu *artigo* 11, *caput* e § 2º:

> Art. 11. **Os documentos produzidos eletronicamente** e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, **serão considerados originais para todos os efeitos legais.**
> (...)
> § 2º **A arguição de falsidade do documento original será processada eletronicamente na forma da lei processual em vigor.**
> § 3º Os originais dos documentos digitalizados, mencionados no § 2º deste artigo, deverão ser preservados pelo seu detentor até o *trânsito em julgado* da sentença ou, quando admitida, até o final do prazo para interposição de ação rescisória. (não há grifos no original)

Como toda prova administrativa ou judicial, a prova digital tem que ser lícita, nos termos do artigo 369 do Código de Processo Civil e deve ser apresentada tempestivamente, sob pena de preclusão. A princípio, deve ser juntada com a inicial ou com a defesa, salvo as exceções previstas em lei, sendo admissível a juntada posterior, por exemplo, quando se tratar de documentos novos, quando destinados a fazer prova "de fatos ocorridos depois dos articulados ou para contrapô-los aos que foram produzidos nos autos", nos termos do artigo 435 do mesmo diploma legal. O parágrafo único desse mesmo artigo assim dispõe:

> Parágrafo único. Admite-se também a juntada posterior de documentos formados após a petição inicial ou a contestação, bem como dos que se tornaram conhecidos, acessíveis ou disponíveis após esses atos, cabendo à parte que os produzir comprovar o motivo que a impediu de juntá-los anteriormente e incumbindo ao juiz, em qualquer caso, avaliar a conduta da parte de acordo com o art. 5º.

Revista ARACÊ
ISSN: 2358-2472

Segundo Thamay e Tamer (2020, p. 40 e 45)., autenticidade é a "qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital". A integridade é "a qualidade da prova digital que permite a certeza com relação à sua completude e não adulteração" e concluem que "Prova digital íntegra, portanto, é aquela não modificada ou adulterada, apta, portanto, a demonstrar a reprodução do fato em sua completude e integridade."

Uma prova digital que tenha sido adulterada não é íntegra, não tendo utilidade para o processo. Didier Jr. et al (2025, p.283), assim dispõe sobre a atribuição da força probatória aos documentos eletrônicos:

> é fundamental avaliar o grau de segurança e de certeza que se pode ter, sobretudo quanto à sua autenticidade, que permite identificar a sua autoria, e à sua integridade, que permite garantir a inalterabilidade do seu conteúdo. Somente a certeza quanto a esses dados é que poderá garantir a eficácia probatória desses documentos.

O profissional do direito tem que ter essa percepção de quais registros digitais de determinado fato podem ser apresentados como prova judicial, bem como saber a forma correta de produzir essa prova nos autos para não correr o risco de alterá-la, observando-se a cadeia de custódia da prova, que é o conjunto de procedimentos de preservação da prova desde o momento de sua coleta até a sua apreciação final.

Muitas provas documentais são apresentadas no processo do trabalho e impugnadas, sendo que as partes, geralmente, pretendem desconstituí-las com depoimentos testemunhais. Podemos citar como exemplos fotos, pedido de demissão e cartões de ponto. Entretanto, a verificação da autenticidade e integridade dos documentos digitais muitas vezes dispensam a produção de prova testemunhal, podendo ser realizada pela análise de seus metadados.

O grande diferencial das provas digitais, além de terem sido extraídas de dispositivos informáticos em comparação às provas documentais contidas em suportes físicos, é sua auditabilidade feita pela análise de seus metadados.

4 METADADOS

Stanton (2012, p. 4 e 11), nos ensina que a Ciência de Dados "refere-se a uma área emergente de trabalho preocupada com a coleta, preparação, análise, visualização, gerenciamento e preservação de grandes conjuntos de informações." A Ciência de Dados tem por objetivo extrair dos dados conhecimento que seja útil para determinado campo de aplicação.

Os dados coletados de dispositivos informáticos podem servir de provas nos processos judiciais, demandando a análise dos requisitos de sua validade, a exemplo de sua autenticidade e

Revista ARACÊ
ISSN: 2358-2472

integridade, ou seja, não adulteração. A análise de dados também pode ser empregada para detectar padrões anômalos que possam indicar fraudes ou outras irregularidades, por exemplo compras por cartão de crédito que destoam do perfil do usuário, efetivadas de um local não usual (geolocalização), possibilitando ações preventivas e corretivas mais rápidas. A análise do número do endereço de IP (Protocolo de Internet) do dispositivo de onde partiu uma postagem ofensiva nas mídias sociais também possibilita a identificação do dispositivo e dos dados cadastrais do usuário da respectiva conexão.

Metadados são dados sobre dados. Segundo Capanema (2024, pág. 196, os metadados "servem para descrever, identificar e qualificar outros. Há uma relação de acessoriedade entre metadados e os dados)".

O Artigo 3, II, do Decreto 10.278/2020 dispõe que metadados são "dados estruturados que permitem classificar, descrever e gerenciar documentos".

Metadados são dados que fornecem informações sobre outros dados. Eles descrevem as características e propriedades dos dados, como formato, autor, data de criação, localização, entre outros atributos. Em outras palavras, são informações que fornecem contexto e ajudam a entender e gerenciar melhor os dados. "A função principal de metadados é descrever o recurso ou objeto informacional de modo a permitir sua identificação, localização, recuperação, manipulação e uso" (CAMPOS, 2007, p.6).

Como exemplo, a capa de um livro contém os metadados sobre seu conteúdo: o título, autor, editora, ano de publicação, etc. O cabeçalho de um e-mail contém seus metadados: remetente, destinatário, assunto, dia e horário de envio. Os arquivos de um texto eletrônico também contêm metadados, como a data e horário da última atualização e o nome do usuário do programa em que foi editado. Vídeos do Youtube® contêm metadados, como data, hora, autor e endereço eletrônico (URL).

Podemos citar como Metadados de Postagens no Instagram e Facebook: data, hora, ID do Autor e URL. Além desses, Capanema (2024, p. 198)., bem destaca como metadados do Instagram®: a "quantidade de interações (curtidas, comentários, 'salvamentos' e compartilhamentos)" e do Facebook®: "quantidade de comentários e curtidas, local da postagem e público da postagem".

A indicação do endereço eletrônico (metadado para identificar um arquivo publicado na internet) é fundamental para requerer judicialmente a exclusão de uma postagem das mídias sociais. Ela deve ser identificada pela URL, nos termos do art. 19, §1º do Marco Civil da Internet, a seguir transcrito:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos

Revista ARACÊ
ISSN: 2358-2472

> decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, **tornar indisponível o conteúdo apontado como infringente**, ressalvadas as disposições legais em contrário.
> § 1º **A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.** (não há grifos no original)

Em uma ação judicial na qual se pleiteia a exclusão de um arquivo de uma página na internet, não adianta falar: "eu quero que exclua a postagem em que fulano me ofendeu". O ilícito deve ser identificado de forma específica. Essa identificação é seu endereço eletrônico, a URL, ou seja, o local em que o objeto apontado será encontrado.

O seguinte Acórdão do Tribunal de Justiça de São Paulo, que teve como Relator o Desembargador Alexandre Coelho, bem ressalta que a indicação do endereço eletrônico é requisito legal para a localização do material que se pretende excluir das aplicações da internet:

> **Tribunal de Justiça do Estado de São Paulo**
> **Agravo de Instrumento nº 2098826-90.2024.8.26.0000**
> **Agravante: Facebook Serviços Online do Brasil Ltda.**
>
> **AGRAVO DE INSTRUMENTO INTERNET INSTAGRAM PROVEDOR DE APLICAÇÃO - POSTAGENS DA IMAGEM DA AUTORA DE TOPLESS TUTELA DE URGÊNCIA DECISÃO QUE DETERMINOU A QUEBRA DO IP E O FORNECIMENTO DOS DADOS DOS RESPONSÁVEIS COM EXCLUSÃO DAS PÁGINAS SOB PENA DE MULTA DIÁRIA DE R$2.500,00 INCONFORMISMO ACOLHIMENTO EM PARTE** – A obtenção das informações tem por objetivo deflagrar a identificação dos ofensores Preenchimento dos requisitos do artigo 22, parágrafo único da Lei 12965/2014 Obrigação dos provedores de acesso de guardar as informações pelo prazo de seis meses **Obrigação, contudo, que não engloba a indicação das URLs Incumbência que cabe ao usuário Inteligência do artigo 19, § 1º, da Lei 12.965/2014** Razoabilidade do valor da multa **Decisão reformada em parte para determinar que a multa aplicada flua somente após a autora fornecer as URLS específicas** DERAM PARCIAL PROVIMENTO AO RECURSO. (não há grifos no original)

5 FERRAMENTAS DE EXTRAÇÃO DE METADADOS

Diversas ferramentas podem ser usadas para extrair e analisar os metadados de dados digitais, como informações de data e hora, localização e dispositivo, para produzir provas digitais. Isso pode incluir análise de metadados de imagens e de arquivos para investigar a origem, integridade e autenticidade do documento.

5.1 PIC2MAP

Uma das ferramentas de extração dos metadados de fotos digitais simples de usar é o Pic2map®. Basta selecionar a foto cujos metadados se pretende analisar e a ferramenta apresentará a

Revista ARACÊ
ISSN: 2358-2472

data, horário e até o tipo de aparelho que tirou a foto. Se o GPS estiver ligado, também trará a geolocalização.

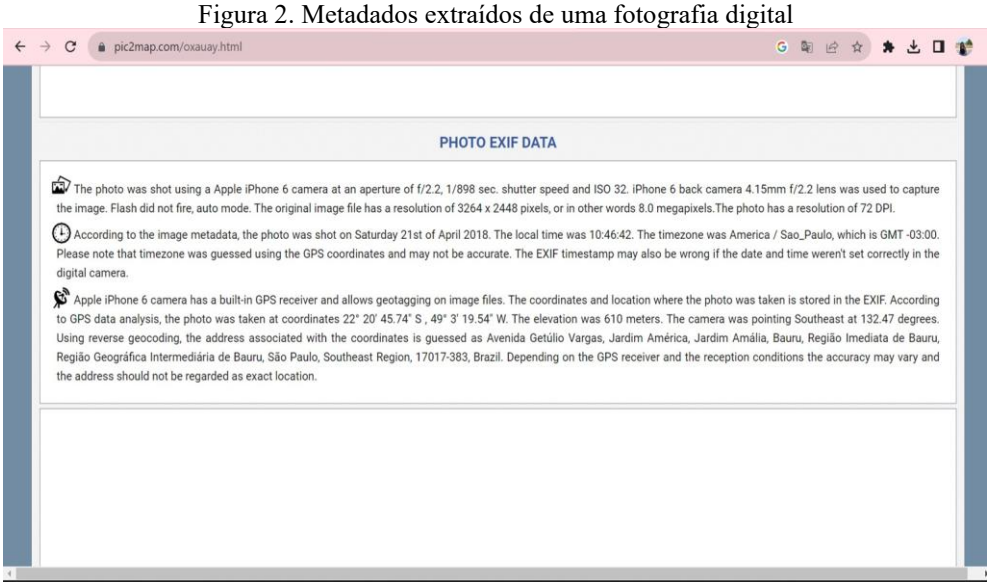
Aqui está um exemplo dos metadados trazidos pelo site pic2map. Esse site mostra todos os metadados de uma foto digital (Figura 1).

Figura 1. Metadados extraídos de uma fotografia digital

Fonte: Metadados extraídos no site Pic2Map.com.

Observa-se, na Figura 2, que não pode ser foto enviada por WhatsApp® ou mídia social, pois os provedores de aplicação retiram os metadados das fotos digitais, quer por questões de privacidade, mas principalmente para reduzir o tamanho dos arquivos.

Figura 2. Metadados extraídos de uma fotografia digital



Fonte: Metadados extraídos no site Pic2Map.com.

Revista ARACÊ
ISSN: 2358-2472

Se a vítima ou alguma câmera de vigilância tirar uma foto do acusado na hora do ilícito, é possível obter os metadados da foto e verificar o horário e local que o acusado estava na hora da foto, através da análise dos metadados (Figura 3).

Figura 3. Metadados extraídos de uma fotografia digital

Fonte: Metadados extraídos no site Pic2Map.com.

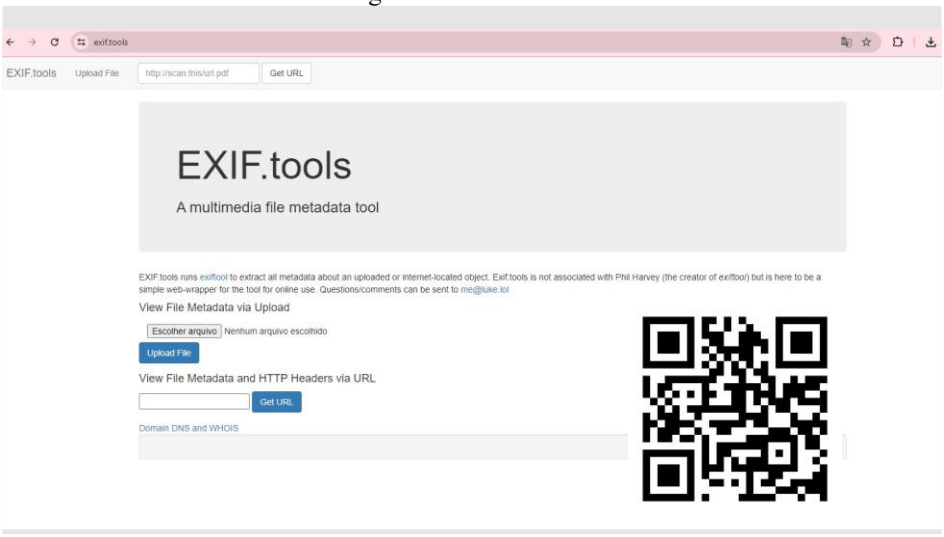
Os metadados de fotografias já têm sido utilizados como forma de comprovar a existência de áreas de vivência na área rural pelos empregadores rurais ou também para comprovar ambientes de trabalho sem as mínimas condições de higiene e conforto, que ferem a dignidade do trabalhador, com fotos dos alojamentos de trabalhadores rurais, por exemplo. Se o empregador juntar fotos com melhorias feitas no alojamento, dá para verificar a data em que a foto foi tirada através da análise de seus metadados.

5.2 EXIF.TOOLS

Outra ferramenta capaz de extrair os metadados de fotos e vídeos é o EXIF.tools (Figura 4), disponível em https://exif.tools/

Revista ARACÊ
ISSN: 2358-2472

Figura 4. Site exif.tools



Fonte: https://exif.tools/ .

EXIF.Tools é um software ou serviço projetado para extrair e analisar metadados EXIF (Exchangeable Image File Format) de fotos. Essa ferramenta permite que os usuários visualizem informações detalhadas incorporadas em imagens digitais, como dados de câmera, configurações de exposição, data e hora em que a foto foi tirada, e até mesmo a localização geográfica, se disponível.

5.3 EXPORTAÇÃO DE MENSAGENS DE WHATSAPP®

Pesquisa do Delegado de Polícia Guilherme Caseli relata a quantidade de dados que trafegam na internet, destacando que a cada 24 horas, 27 bilhões de mensagens são enviadas via WhatsApp®. (2022, p. 43). Esses dados explicam por que a reprodução de mensagens de WhatsApp é o meio de prova digital mais comum nos processos do trabalho, justamente porque é o meio de comunicação digital mais utilizado.

Um captura de tela do WhatsApp® é apenas um arquivo de imagem, ou seja, é uma foto digitalizada, que não contém metadados, ou seja, não é auditável. Para que ela seja auditável, deve ser feita a exportação das mensagens com os respectivos metadados, cujo arquivo deverá ser juntado aos autos do processo judicial.

Os metadados de uma conversa de WhatsApp® podem ser obtidos ao se clicar no nome da pessoa ou do Grupo das mensagens que se pretende apresentar e “rolar a tela para baixo no smartphone tipo iPhone” ou clicar nos três pontinhos no aparelho com sistema operacional Android, devendo, em ambos, escolher a opção “exportar conversa”, com ou sem mídia. Depois, basta escolher o local para onde se deseja que o arquivo exportado seja enviado. Um arquivo exportado do WhatsApp® contém

Revista ARACÊ
ISSN: 2358-2472

a data, horário, nome do interlocutor e as mensagens trocadas, inclusive constando data e horário de mensagens, arquivos de fotos e áudios que foram apagados.

5.4 ENDEREÇOS DE IP (PROTOCOLO DA INTERNET)

Um dos principais metadados para comprovação da autenticidade de uma prova digital, ou seja, da autoria de quem acessou uma aplicação da internet (postagem em mídias sociais, envio de e-mail, mensagens em aplicativos de mensageria, compras pela internet, transações financeiras, aplicativos de transporte etc.) é o endereço de IP (Internet Protocol ou Protocolo de Internet).

O Marco Civil da Internet (Lei 12.965/2014), em seu artigo 5º, III, define o endereço de protocolo de internet (endereço IP) como: *"o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais"*

O acesso à internet é feito através de um Provedor de Conexão (Vivo, Tim, Claro, Net, etc), que são sistemas autônomos. O provedor de conexão nos dá o acesso à internet através de uma chave, um código, chamado de IP (Internet Protocol). Cada vez que alguém, se conecta à internet é gerado um número de IP.

É o IP que diferencia um usuário de internet de outro, ainda que utilizem computadores, celulares e dispositivos do mesmo modelo. Ninguém é anônimo na internet. Quando ocorre a conexão de um dispositivo informático à Internet, um endereço de IP (Internet Protocol) é atribuído exclusivamente para aquele dispositivo. Não existem dois dispositivos com o mesmo IP durante a navegação na internet (no mesmo dia, hora e fuso horário).

Os provedores de aplicação à internet têm o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de seis meses. Essa obrigação, quanto aos provedores de conexão, é pelo prazo de um ano, nos termos da Lei nº 12.965/2014 (Marco Civil da Internet). Assim, obtido o IP do dispositivo que fez determinada publicação nas mídias sociais (considerando-se o dever de guarda pelo prazo de seis meses), ainda haverá o prazo de mais seis meses para obter junto ao Provedor de Conexão os dados cadastrais de referido autor.

O endereço de IP (Protocolo da Internet) e a geolocalização (local em que se encontrava o terminal – dispositivo informático) captados durante as transações financeiras efetuadas por aplicações da internet é uma medida de segurança utilizada pelas instituições financeiras. Ao aderir aos termos de uso dos aplicativos bancários, consente-se em compartilhar o endereço de IP a geolocalização com a instituição bancária.

A prova da geolocalização no momento da contratação de um empréstimo ou outra transação financeira e o perfil do cliente é fundamental para comprovar a responsabilidade da instituição

Revista ARACÊ
ISSN: 2358-2472

financeira em caso de transações fraudulentas em nome do cliente. Nesse sentido o Acórdão do Tribunal de Justiça do Estado de São Paulo, que teve como Relator o Desembargador Sídney Braga, proferido em 24/05/2024:

> **APELAÇÃO CÍVEL**
> **Processo nº 1016397-55.2022.8.26.0032**
> **Comarca: Araçatuba (4ª Vara Cível)**
> **Apelante: ANTÔNIO APARECIDO DE MELO**
> **Apelado: BANCO SANTANDER (BRASIL) S/A**
>
> AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE NEGÓCIO JURÍDICO CC. INDENIZAÇÃO POR DANOS MORAIS - Empréstimo consignado - **Autor que comprovou a inclusão do débito em seu benefício previdenciário, negando, todavia, a celebração do contrato - Réu que não trouxe aos autos documentos suficientes para comprovar a relação jurídica entre as partes** - Contrato firmado de forma digital que, em regra, é válido - Caso concreto - **Instrumento desacompanhado dos dados básicos de registro digital da transação, os chamados metadados - *Selfie* e cópia de documento pessoal que, desacompanhados dos dados de registro usualmente captados neste tipo de transação eletrônica (ID do dispositivo eletrônico, IP e geolocalização do usuário) não servem para vincular válido aceite ao negócio - Contrato que deve ser declarado inexistente** - Devolução em dobro dos valores indevidamente descontados em benefício previdenciário - **Requerido que, no mínimo, agiu com culpa na modalidade negligência, ao deixar de armazenar os dados de registro digital, afastando sua boa-fé objetiva** - Dobra do art. 42, parágrafo único, do CDC aplicável - Danos morais configurados - Privação de verba de caráter alimentar - Valor arbitrado em R$ 5.000,00 - Precedentes desta C. Câmara - Sentença reformada - Demanda procedente.
> Dá-se provimento ao recurso.(não há grifos no original)

Se uma foto ou vídeo é postado no Instagram®, Facebook® ou Youtube®, o metadado é o ID de seu autor e o endereço de IP (protocolo da Internet), sendo possível, diante de um suposto ilícito, oficiar judicialmente ao Provedor de Aplicação requisitando-se o número do IP do dispositivo que realizou a postagem. Com esse número, oficia-se ao Provedor de Conexão, solicitando-se os dados cadastrais da pessoa a quem foi atribuído aquele IP.

6 MOMENTO DA APRESENTAÇÃO DOS METADADOS

Em se tratando de prova digital (fotos digitais, e-mails, postagens feitas nas mídias sociais, mensagens em aplicativos de mensageria), a quem compete comprovar sua autenticidade (autoria) caso tenha sido impugnada?

Questiona-se qual o momento para apresentação dos metadados da prova digital no processo judicial. Os metadados devem ser apresentados junto com a prova digital (com a inicial ou com a contestação) sob pena de preclusão e inversão do ônus da prova ou podem ser apresentados posteriormente, caso seja impugnada a autenticidade da prova digital?

Revista ARACÊ
ISSN: 2358-2472

O Código Civil, em seu artigo 225 estabelece que as "reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão."

O Código de Processo Civil estabelece algumas normas quanto aos documentos eletrônicos:

> Art. 411. Considera-se autêntico o documento quando:
> (...)
> II - a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei;
> III - não houver impugnação da parte contra quem foi produzido o documento.

Já o artigo 422, *caput*, do CPC estabelece que as reproduções mecânicas ou de outra espécie têm aptidão para fazer prova dos fatos ou das coisas representadas, se a sua conformidade com o documento original não for impugnada por aquele contra quem foi produzida.

O parágrafo 1º do artigo 422 aplica a mesma regra às fotografias digitais e as extraídas da internet, imputando a quem as produziu, caso sejam impugnadas, o ônus de apresentar sua "autenticação eletrônica". Caso não seja possível comprovar sua autenticidade seria necessária a realização de perícia.

Capanema (2024, p.207) ressalta que a legislação processual não determinou requisitos de validade para a prova digital:

> "A sua validade só será analisada em eventual impugnação da parte contra a qual é produzida, por meio da arguição de falsidade (arts. 430 a 433, CPC e art. 11, § 2, Lei 11.419/2006)".

O art. 429 do CPC assim dispõe:

> Incumbe o ônus da prova quando:
> I - se tratar de falsidade de documento ou de preenchimento abusivo, à parte que a arguir;
> II - se tratar de impugnação da autenticidade, à parte que produziu o documento.

Diante dos dispositivos legais supratranscritos, a princípio, os documentos devem ser juntados com a inicial ou junto com a defesa, sob pena de preclusão, nos termos dos artigos 320 e 434 do CPC. Entretanto, nos termos do artigo 422 do CPC, em se tratando de documento digital, caso seja impugnado, cabe à parte que o produziu comprovar sua autenticidade, sendo, portanto, admitido à parte apresentar metadados ou outro meio que comprove a certificação eletrônica do documento apresentado.

Em síntese, uma vez impugnada, cabe à parte que apresentou a prova digital comprovar sua autenticidade e integridade, sendo possível apresentar novos documentos (metadados) para fazê-lo,

Revista ARACÊ
ISSN: 2358-2472

nos termos dos artigos 422, § 1º e 435 do CPC. Caso não sejam juntados os metadados da prova digital, inverte-se o ônus da prova quanto ao fato que com ela se pretendia provar.

7 CONCLUSÃO

O Brasil é um dos países onde as pessoas passam mais tempo conectadas na internet, seja pelo celular ou computador, o que foi intensificado pela pandemia. Nessa sociedade da informação, praticamos muitos atos de forma digital, principalmente através do aparelho celular, estando o tempo todo conectados. Deixamos rastros digitais por onde navegamos e nem percebemos, os quais podem ser muito úteis como prova em processo judicial.

Na era digital, a produção de provas em processos administrativos ou judiciais passa a incluir uma vasta gama de registros eletrônicos, desde e-mails, postagens nas mídias sociais, geolocalização e mensagens instantâneas até dados de sistemas de gestão de recursos humanos.

O grande diferencial das provas digitais, além de terem sido extraídas de dispositivos informáticos em comparação às provas documentais contidas em suportes físicos, é sua auditabilidade feita pela análise de seus metadados.

Como se procurou evidenciar neste artigo, os metadados funcionam como uma assinatura digital invisível, um registro técnico que permite rastrear a origem, a autoria e o histórico de um arquivo. Diversas ferramentas podem ser usadas para extrair e analisar os metadados de provas digitais, como informações de data e hora, localização e dispositivo.

O profissional do direito tem que ter essa percepção de quais registros digitais de determinado fato podem ser apresentados como prova judicial, bem como saber a forma correta de produzir essa prova nos autos, inclusive com os respectivos metadados para comprovar sua autenticidade e integridade.

Caso pairem dúvidas sobre a validade de uma prova digital, uma vez impugnada, cabe à parte que apresentou a prova digital comprovar sua autenticidade e integridade, sendo possível apresentar novos documentos (metadados) para fazê-lo, nos termos dos artigos 422, § 1º e 435 do CPC. Caso não sejam juntados os metadados da prova digital, inverte-se o ônus da prova quanto ao fato que com ela se pretendia provar.

A análise de metadados tornou-se essencial para verificar a autenticidade e integridade das provas, garantindo maior precisão e confiabilidade nos processos judiciais. Quanto mais metadados disponíveis (autoria, origem, data, IP etc.), maior o grau de confiabilidade da prova.

A integração da tecnologia ao Direito do Trabalho não apenas aprimorou a produção e análise de provas, tornando-a mais assertiva, mas também contribui para a pacificação social e efetividade do

Revista ARACÊ
ISSN: 2358-2472

direito, alinhando-se com os Objetivos de Desenvolvimento Sustentável (ODS) da Agenda 2030 da ONU (2015), notadamente a ODS 16 (promover sociedades pacíficas e inclusivas, garantir o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas.) e a ODS 9 (a qual incentiva investimentos em pesquisa e desenvolvimento e a ampliação do acesso à internet como forma de reduzir desigualdades) as quais representam pilares fundamentais para a construção de sociedades mais justas e resilientes.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

BERNERS-LEE, Tim; FIELDING, Roy; MASINTER, Larry. Uniform Resource Locators (URL). Request for Comments RFC 1738. Internet Engineering Task Force, dez. 1994. Disponível em: <https://tools.ietf.org/html/rfc1738>. Acesso em: 15 out. 2024.

BRASIL, LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 out. 2023.

BRASIL, LEI Nº 13.105, DE 16 DE MARÇO DE 2015. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em 1 set. 2024.

CAMPOS, L. F. de B. (2007). Metadados digitais: revisão bibliográfica da evolução e tendências por meio de categorias funcionais. Encontros Bibli: Revista eletrônica De Biblioteconomia e Ciência da informação, 12(23), 16-46. Disponível em https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2007v12n23p16/390. Acesso: 1 set. 2024.

CAPANEMA, Walter Aranha. Curso de Provas Digitais, 2023. SMART3. Disponível em: https://smart3.eadplataforma.app/curso/curso-de-provas-digitais-66cea8f405e11. Acesso em: 1 set. 2024.

CAPANEMA, Walter Aranha. Manual de Direito Digital. São Paulo: Editora JusPodivm, 2024.

CASELLI, Guilherme. Manual de Investigação Digital. São Paulo: Editora JusPodivm, 2022.

DIDIER Jr, Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. Curso de Direito Processual Civil – v.2. Teoria da prova, direito probatório, decisão, precedente, coisa julgada, processo estrutural e tutela provisória. São Paulo: Editora JusPodivm, 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Transformando nosso mundo: a Agenda 2030 para o desenvolvimento sustentável. Nova York: ONU, 2015. Disponível em: https://vocepergunta.com/library/artigo/read/125632-como-referenciar-a-agenda-2030. . Acesso em: 15 out. 2024.

SCHIAVI, Mauro. Manual de Direito Processual do Trabalho. Salvador: Editora JusPodivm. 2021.

STATON, J.M. (2012). Introduction to Data Science, Third Edition. iTunes Open Source eBook, 2012. Disponível em: HYPERLINK "https://itunes.apple.com/us/book/introduction-to-data-science/id529088127?mt=11". Acesso em: 10 out. 2023..

THAMAY, Rennan e TAMER, Mauricio. Provas no Direito Digital: conceito da prova digital, procedimentos e provas digitais em espécie, São Paulo: Thomson Reuters Brasil, 2020.

Exif.tools. Disponível em HYPERLINK "https://exif.tools/"https://exif.tools/. Acesso em: 1 set. 2024..

Revista ARACÊ
ISSN: 2358-2472

Pic2Map.com. Disponível em: https://www.pic2map.com/. Acesso em: 1 set. 2024.Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento nº 2098826-90.2024.8.26.0000. Relator Desembargador Alexandre Coelho. Julgado em 29.05.24. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=17945908&cdForo=0. Acesso em: 1 set. 2024.

Tribunal de Justiça do Estado de São Paulo. Processo nº 1016397-55.2022.8.26.0032. Relator Desembargador Sidney Braga. Julgado em 24/05/2024. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=17930553&cdForo=0. Acesso em: 1 set. 2024.