WALTER ARANHA
CAPANEMA

Manual de
DIREITO DIGITAL

Teoria e Prática

3ª edição
Revista, Atualizada e Ampliada

2026

EDITORA JusPODIVM
www.editorajuspodivm.com.br

5

PROVAS DIGITAIS

1. PROVAS DIGITAIS

1.1. Introdução. Conceito

Rennan Thamay e Mauricio Tamer apresentam duas acepções de prova digital: "(u)ma primeira, segundo a qual a prova digital pode ser entendida como a demonstração de um fato ocorrido nos meios digitais, isto é, um fato que tenha como suporte a utilização de um meio digital. E, uma segunda, em que, embora o fato em si não tenha ocorrido em meio digital, a demonstração de sua ocorrência pode se dar por meios digitais" [1].

Essa provas se apresentam na forma de documentos, em duas espécies:

a) **Documentos digitais ou digitalizados,** hospedados em arquivos, *localmente*, em discos rígidos ou mídias externas (*pendrives*, hds externos e cartões SD[2], por exemplo) ou, ainda, armazenados remotamente em servidores ou sistemas de nuvem;

b) **Resultado da interceptação telemática**: são os pacotes de dados trocados entre dois ou mais dispositivos, que foram

1. THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 32.
2. SD é a sigla de "*Security Digital*". Trata-se de um formato de cartões de armazenamento para câmeras e smartphones, introduzido no mercado em 1999. PCMag. **SD card**. Disponível em: https://www.pcmag.com/encyclopedia/term/sd-card. Acesso em: 14 ago. 2022.

> copiados por meio de interceptação telemática. São, portanto, os arquivos que estavam circulando entre uma comunicação e foram "grampeados", nos termos da Lei 9.296/96.

Há relevância jurídica nessa diferenciação, pois cada uma dessas espécies de provas digitais possui bases legais e requisitos formais próprios.

Tais provas podem ser constituídas pela vontade humana, como, por exemplo, os *e-mails*, ou mediante a intervenção automatizada de sistemas de computadores, o que ocorre com os registros de conexão, que surgem quando um usuário se conecta à internet (art. 13, Marco Civil da Internet).

Tais provas constituem o denominado "**direito probatório de 3ª geração**", que abarca as tecnologias extremamente invasivas, as quais permitem que as autoridades investigativas obtenham muito mais informações do que pelos meios tradicionais normalmente utilizados[3]. Há a possibilidade de obtenção de provas em maior quantidade e melhor qualidade.

A utilização de provas digitais não é um fenômeno recente e precede a popularização da Internet comercial. Já em 1984, o FBI desenvolvia programas para análise de arquivos[4]. Dan Farmer e Wietse Venema, considerados pioneiros na área da computação forense, criaram em 1999 o programa "*The Coroner's Toolkit*" para análise pericial de sistemas Linux.[5]

O tema é profundamente desafiador, não só pela escassa doutrina existente, mas também pela ausência de uma sistematização normativa.

---

3. A 1ª geração do direito probatório, denominada de "teoria proprietária", tem como base o julgado da Suprema Corte dos EUA – SCOTUS *Olmstead v. United States* (1928), o qual estabeleceu que a proteção constitucional para buscas e apreensões está limitada à áreas que podem ser objetivamente demarcadas. Já a 2ª geração, que trata da "teoria da proteção constitucional integral", surgiu com a decisão da SCOTUS em *Katz v. United States (1967)*, que ampliou aquela proteção para lugares onde o indivíduo tivesse razoável expectativa de privacidade ("*reasonable expectation of privacy*"). KNIJNIK, Danilo. A trilogia Olmstead-Katz-Kyllo**:** o art. 5º da Constituição Federal do século XXI. **Revista da Escola da Magistratura do TRF da 4ª Região**, ano 2, número 4. Porto Alegre/RS, 2016. BIFFE JUNIOR, João; LEITÃO JUNIOR, Joaquim. O acesso pela polícia a conversas gravadas no WhatsApp e as gerações probatórias decorrentes das limitações à atuação estatal. **Revista do Ministério Público do Estado de Goiás**, Goiânia, v. 21, n. 32, p. 9-30, jul. 2016.

4. Federal Bureau of Investigation. **Recovering and Examining Computer Forensic Evidence**. Disponível em: bit.ly/43EcyBG. Acesso em: 23 fev. 2021.

5. VENEMA, Wietse. **The Coroner's Toolkit (TCT).** Disponível em: http://www.porcupine.org/forensics/tct.html. Acesso em: 23 fev. 2021.

Além disso, há uma quantidade praticamente infinita de provas digitais criadas por aplicativos, redes sociais e sites da Internet.

1.2. Normas jurídicas e técnicas aplicáveis

Não há uma lei que trate especificamente das provas digitais. Há regramentos pontuais em diversas normas, podendo-se aqui destacar as seguintes:

a) **Decreto-Lei 3.689/1941 (Código de Processo Penal), com a alteração da Lei 13.344/2016**: em tipos penais específicos[6], admite a requisição de dados cadastrais (eletrônicos ou não) de suspeitos (art. 13-A); e mediante autorização judicial, de informações de empresas prestadoras de serviço de telecomunicações e/ou telemática (art. 13-B) que permitam a localização da vítima ou dos suspeitos do delito em curso;

b) **Lei 8.069/1990 (Estatuto da Criança e do Adolescente), com a alteração da Lei 13.441/2017**: infiltração de agentes de polícia na internet (art. 190-A a 190-E).

c) **Lei 9.296/1996:** estabelece o procedimento das interceptações telefônicas e telemáticas;

d) **Lei 9.472/1997 ("Lei da ANATEL"):** divulgação de dados pessoais de usuário de telefonia (art. 72);

e) **Lei 9.613/1998, com a alteração da Lei 12.683/2012:** acesso aos dados cadastrais pela autoridade policial e o Ministério Público (art. 17-B);

k) **Lei 10.406/2002 (Código Civil):** reproduções eletrônicas (art. 225);

f) **Lei 10.703/2003:** acesso à dados de cadastro de usuário de telefone celular pré-pago (art. 1º, § 3º);

g) **Lei 11.419/2006 (Lei do Processo Eletrônico)**: documentos eletrônicos (art. 11) e arguição de falsidade (art. 11, § 2º);

6. No caso do art. 13-A: crimes previstos nos arts. 148, 149 e 149-A, do art. 158, no § 3º e no art. 159 do Código Penal, bem como no art. 239, ECA.
Já no art. 13-B, o delito de tráfico de pessoas.

h) **Lei 12.965/2014 (Marco Civil da Internet):** acesso às comunicações privadas armazenadas (art. 10) e aos dados cadastrais (art. 10, § 3º); guarda e acesso de registros de conexão e de aplicação (arts. 13 e 15), requisição judicial de registros (arts. 22 e 23);

i) **Lei 13.105/2015 (Código de Processo Civil):** documentos eletrônicos (arts. 439 a 441);

j) **Decreto 8.771/2016:** regulamenta o Marco Civil da Internet, especialmente do que tange à requisição de dados cadastrais pelas autoridades administrativas (arts. 11 e 12);

Há, por outro lado, outras normas que, muito embora não digam respeito às provas digitais, **repercutem**, em sua produção, ao, por exemplo, exigir a organização escritural e documental de uma empresa, ou estabelecer o dever de produzir e armazenar determinados documentos.

O caso mais emblemático é o da Lei Geral de Proteção de Dados, que determina o dever do controlador e do operador de manterem registro das atividades de tratamento de dados pessoas que forem realizar (art. 37). Tal dever busca atender aos princípios da transparência (art. 6º, VI) e da responsabilização e prestação de contas (art. 6º, X). Esses registros, que são, na verdade, documentos, podem, ser eventualmente utilizados como prova em processos administrativos, arbitrais e judiciais. A LGPD exige que as instituições promovam uma organização interna de seus documentos, o que facilitará uma eventual produção probatória.

O Decreto 7.962/2013, que regulamenta o Código de Defesa do Consumidor nas relações de comércio eletrônico, prevê uma série de deveres aos fornecedores, notadamente os de manter em seu sítio eletrônico informações detalhadas sobre a sua constituição (nome empresarial, CPF ou CNPJ, endereço físico e eletrônico etc – art. 2º, I e II), e sobre as ofertas (art. 2º, incisos III a VI).

Cabe ao fornecedor, dentre outras atribuições, apresentar ao consumidor um sumário do contrato antes da sua conclusão (art. 4º, I) e, após, o seu inteiro teor (art. 4º, IV); confirmar a conclusão do contrato (art. 4º, III) e comunicar o recebimento da manifestação de arrependimento (art. 5º, § 4º).

Quanto às normas de caráter **técnico**, podem-se destacar as seguintes:

a) **ISO 27037**: "Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais"[7];

b) **RFC 3227**: "Diretrizes para Coleta e Arquivamento de Evidências".[8]

1.3. Classificação das provas digitais

Torna-se fundamental estabelecer uma classificação das provas digitais, de forma a facilitar a sua compreensão e o seu uso na prática. Uma categorização adequada pode ser útil tanto para as partes como para os próprios juízes, permitindo que sejam identificadas com mais facilidade as particularidades e limitações de cada uma das suas espécies.

a) Quanto à necessidade de ordem judicial para o seu acesso ou para a sua formação: há provas digitais que *dependerão de decisão judicial para o seu acesso*, como os registros de conexão e aplicação (art. 10, § 1º, Marco Civil) e as comunicações armazenadas (art. 10, § 2, Marco Civil). Outras exigirão ordem judicial para a sua *formação*, como as interceptações telemáticas (Lei 9.296/96), as quais só serão obtidas por meio de um procedimento tecnológico que permitirá a coleta dos dados de determinada comunicação.

Há ainda as provas que *independem de ordem judicial para o seu acesso ou formação*, que são, por exemplo, as disponíveis em fontes abertas, como as redes sociais e sites da Internet, em que normalmente o próprio investigado/réu/parte a produz de forma espontânea.

Há provas digitais que, dependendo do cargo ou função exercidos pelo solicitante, não precisará da exigência de ordem judicial. De acordo com a jurisprudência do STJ (HC n. 626.983), os dados pessoais cadastrais dos usuários de internet (qualificação pessoal, filiação e endereço)

7. Disponível (mediante pagamento de taxa) em https://www.iso.org/standard/44381.html
8. Disponível em https://www.ietf.org/rfc/rfc3227.txt

poderão ser acessados diretamente pelas autoridades administrativas e policiais e o Ministério Público.

b) Quanto ao estado dos dados: há provas referentes à *dados estanques*, ou seja, armazenadas em locais específicos, como computadores, servidores ou *tablets*, e aquelas relativas *à dados em movimento / em trânsito*, em que as provas são a coleta de pacotes de dados de uma comunicação telemática em trâmite. O legislador constituinte escolheu por conferir maior proteção a esta última, exigindo que o acesso ao conteúdo dessas comunicações ocorra apenas nos casos da persecução penal, e após ordem judicial específica (art. 5º, XII, CF).

c) Quanto aos dados reciprocamente considerados: a inspiração é notadamente a classificação civilista de bens "reciprocamente considerados", onde há a existência de bens principais e acessórios. Aqui, há provas digitais que se referem à *dados* propriamente ditos. São informações contidas em arquivos de computador, documentos ou em pacotes de fluxos de comunicação.

Há, também, os *metadados*[9], que servem para que descrever, identificar e qualificar outros. Há uma relação de acessoriedade entre os metadados e os dados.

Há um conceito normativo de metadados no art. 3º, II, Decreto 10.278/2020: são "dados estruturados que permitem classificar, descrever e gerenciar documentos".

Elkind, Gillium e Silverman apresentam uma interessante analogia:

> "metadado é o equivalente ao que está escrito do lado de fora de um envelope – os nomes e endereços do remetente e do destinatário e o carimbo do correio informando onde e

9. "O prefixo "Meta" vem do grego e significa "além de". Assim Metadados são informações que acrescem aos dados e que têm como objetivo informar-nos sobre eles para tornar mais fácil a sua organização. Um item de um metadado pode informar do que se trata aquele dado numa linguagem inteligível para um computador. Os metadados tem a função de facilitar o entendimento dos relacionamentos e evidenciar a utilidade das informações dos dados". SAFERNET. **O que são os Metadados?** Disponível em: https://new.safernet.org.br/content/o-que-s%C3%A3o-os-metadados#. Acesso em: 1 mar. 2021.

quando foi enviado – enquanto o "conteúdo" [os dados] é o conteúdo da carta"[10].

Figura 44: Exemplos de metadados de um arquivo do Microsoft Word

Na presente tabela, se resumiu os principais dados, acompanhados dos seus respectivos metadados:

Dado	Exemplos de metadados:
Arquivo de Computador	Nome, data de criação e modificação, geolocalização, autor e tamanho
Conexão telemática	Número IP, data e hora, porta lógica, Fuso horário

10. ELKIND, Peter; GILLUM, Jack; SILVERMAN, Craig. **How Facebook Undermines Privacy Protections for Its 2 Billion WhatsApp Users**. Disponível em: https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users. Acesso em: 21 fev. 2023.

Dado	Exemplos de metadados:
E-mail	Cabeçalho (data e hora de envio e recebimento, remetente e destinatário)
URL	Parâmetros como a origem do compartilhamento, o tipo de dispositivo usado ou o código identificador do usuário
Vídeo do Youtube	Título, autor, data da postagem, quantidade de visualizações e de comentários, curtidas, resolução do vídeo
Foto do Instagram	Autor, data da postagem, quantidade de interações (curtidas, comentários, "salvamentos" e compartilhamentos)
Post do Facebook	Autor, data e hora da postagem, quantidade de comentários e de curtidas, local da postagem e público da postagem
Tweet do X	Autor, data e hora da postagem, quantidade de comentários, *retweets* e curtidas e local
Vídeo do TikTok	Autor, data da postagem, quantidade de curtidas e de comentários
Non Fungible Token (NFT)	Nome e descrição[11]

Um dado para existir não precisa, necessariamente, dos seus metadados. Os aplicativos e serviços da família *Meta* (incluindo o *Instagram* e o *WhatsApp*) "limpam" os metadados do conteúdo a ser enviado[12], sob a alegação de proteger a privacidade de seus usuários. Contudo, descobriu-se que o próprio Facebook adiciona

11. SINGH, Jagjit. **How to find your NFT's metadata?** Disponível em: https://cointelegraph.com/news/how-to-find-your-nft-s-metadata. Acesso em: 1 set. 2022.

12. A "limpeza dos metadados" também é realizada pelos sites Craigslist, Ebay, Imgur e Twitter, dentre outros. A plataforma de blogs Tumblr, por exemplo, não apaga os metadados. GERMAIN, Thomas. **How a Photo's Hidden 'Exif' Data Exposes Your Personal Information.** Disponível em: https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/. Acesso em: 8 jun. 2021. KUKSOV, Igor. **Do your online photos respect your privacy?** Disponível em: https://www.kaspersky.com/blog/exif-privacy/13356/. Acesso em: 8 jun. 2021.

metadados nas fotos, de modo a identificar qual usuário realizou o seu *download*[13].

Ou seja, as informações contidas nos metadados podem ser suprimidas ou até mesmo substituídas ("falsificadas").

Nos arquivos, os metadados costumam estar inseridos em seu conteúdo, em uma parte específica ou ainda em um cabeçalho. Podem, todavia, ficar em documento ou local destacado do conteúdo principal, como, por exemplo, os registros de conexão.

Caselli classifica os metadados em três espécies[14]:

a) **descritivos**: apresentam informações que permitem individualizar o dado (título da obra, seu autor, resumo etc.);

b) **estruturais**: informam como um dado é constituído ou organizado (capítulos, tipos de arquivos etc.);

c) **administrativos**: são utilizados para atividades de gerenciamento, dizendo respeito às datas de criação ou de aquisição de um arquivo e suas permissões de acesso, dentre outras.

Existe um padrão de metadados próprio para arquivos de mídia. É o denominado *Exchangeable Image File Format* – EXIF ("Formato de Arquivo de Imagem Intercambiável"), o qual armazena, por exemplo, as seguintes informações: data e hora, geolocalização (se ativada no dispositivo), informações do dispositivo (modelo e fabricante) e detalhes das configurações[15]. Tais informações podem ser lidas em sites como o *Metadata2Go*[16] (imagens) e aplicativos como o *ExifTool*[17] (diversos) e o *Geosetter* [18](geolocalização em imagens).

---

13. DOFFMAN, Zak. **Facebook Embeds 'Hidden Codes' To Track Who Sees And Shares Your Photos**. Disponível em: bit.ly/3qIdaI9. Acesso em: 8 jun. 2021.
14. Trata-se do controle de alcance do conteúdo que é feito pelo usuário. Pode-se definir que um *post* tenha um alcance "público", em que qualquer pessoa pode ter acesso, para até o "somente eu", em que as informações ficam disponíveis apenas para o respectivo criador.
15. COSSETTI, Melissa Cruz. **O que são dados EXIF de fotos e como encontrá-los ou escondê-los.** Disponível em: https://tecnoblog.net/259798/o-que-sao-dados-exif-de-fotos-e-como-encontra-los-ou-esconde-los/. Acesso em: 8 jun. 2021.
16. Disponível em https://www.metadata2go.com/.
17. Disponível em https://exiftool.org/.
18. Disponível em https://geosetter.de/en/main-en/.

Portanto, é importante ressaltar que existem metadados não apenas nos dados de nossos computadores e dispositivos informáticos, mas em grande parte da Internet, e até mesmo nas URLs.

É possível a inserção de parâmetros opcionais nas URLs[19], que podem servir para customizar a navegação do usuário ou, ainda, para identificar a existência de compartilhamento, como no exemplo abaixo:

https://www.instagram.com/p/
Ch5h-fGLz1k/**?utm_source=ig_web_button_share_sheet**

O parâmetro em destaque (a partir do ?utm) informa que o link, referente a uma postagem no Instagram, foi compartilhado a partir do botão "*share*" via web.

Aqui o parâmetro aponta para a informação de que o conteúdo foi compartilhado a partir da opção "copiar link" via web:

https://www.instagram.com/p/
Ch5h-fGLz1k/**?utm_source=ig_web_copy_link**

No X, o parâmetro "s=" informa o tipo de dispositivo de onde se originou o compartilhamento do link: "s=19" se refere à *smartphones* Android; "s=20", ao uso da versão Web e "s=21" à aparelhos que usam o sistema iOS, como o iPhone[20]:

https://twitter.com/daniel_eckler/
status/1572210382944538624?t=kBrsV8HKUFeWtpRFWmf1dQ**&s=19**

19. FASTSPRING. **Using Optional Parameters.** Disponível em: https://fastspring.com/docs/classic/using-optional-parameters/. Acesso em: 30 ago. 2022.
20. Muitos desses parâmetros são descobertos pelo uso da ferramenta unfurl, disponível em https://dfir.blog/unfurl/.

Sempre que o ChatGPT apresenta uma fonte para um texto que tenha produzido, ele insere um metadado na URL:

https://www.proofpoint.com/us/threat-reference/deepfake?utm_source=chatgpt.com

Verificou-se em *smartphones* da marca Samsung, e que rodam o sistema operacional Android, uma interessante forma de metadados em arquivos originários de "*print screen*":

Figura 45: Detalhes do nome de arquivo de um "print" de um smartphone Samsung

O sistema, ao criar o arquivo com o "*print*", insere, em seu nome, a indicação de onde foi coletado:

Screenshot_ano mês dia – hora minuto segundo_app de onde saiu o print.jpg

Foi possível identificar a presença de metadados em imagens criadas por ferramentas de Inteligência Artificial Generativa. As principais empresas do setor, como OpenAI, Adobe e Microsoft, inserem campos específicos nesses metadados para garantir transparência e informar os usuários sobre a origem das imagens.

Ao analisar os metadados de imagens criadas pelas principais ferramentas de IA generativa com o site Metadata2go, verificou-se que essas ferramentas geralmente inserem as informações no campo "**claim_generator**" dos metadados.

Um exemplo de metadado de uma imagem gerada pelo Microsoft Copilot:

c2_pa_actions_salt	722613e34f066bb7c6c4e02b3bf6cecf
actions_software_agent	Image Creator from Designer ←
actions_when	2024-11-16T03:00:21Z
actions_digital_source_type	http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia
actions_description	AI Generated Image ←
actions_action	c2pa.created
format	image/jpeg
signature	self#jumbf=c2pa/urn:uuid:c329debd-6007-49b5-a1f8-a5ca438e7872/c2pa.signature
instance_id	1
claim_generator	Microsoft_Responsible_AI/1.0 ←
claim__generator__info_name	Microsoft Responsible AI Image Provenance ←

Figura 45: Metadados do Copilot 1

Ao analisar as principais ferramentas de IA generativa, é possível identificar os principais campos que fornecem informações sobre sua origem sintética:

Ferramenta	Campo de Metadado	Conteúdo do Campo
Adobe Firefly	claim_generator	"Adobe_Firefly"
Adobe Firefly	Title	"Generated Image"
Microsoft Copilot / Bing Images	actions_software_agent	"Image Creator from Designer"
Microsoft Copilot / Bing Images	action_description	"AI Generated Image"
Microsoft Copilot / Bing Images	claim_generator_info_name	"Microsoft Responsabile AI image Provenance"
Microsoft Copilot / Bing Images	claim_generator	"Microsoft Responsible_AI"
OpenAI Dall-E	claim_generator	"OpenAI-API"
OpenAI Sora	actions_software_agent	"Sora"

Há um erro muito comum de considerar os metadados provas de pouca relevância. O ex-diretor da NSA, Michael Hayden, chegou a afirmar que o governo americano "mata pessoas com base em metadados"[21].

Quando o empresário americano John McAfee, criador da empresa de antivírus que leva o seu nome, fugiu do seu domicílio em Belize, devido a uma acusação de homicídio, este foi localizado por um repórter da revista *Vice*, que realizou uma longa entrevista com o milionário. O texto da matéria foi disponibilizado no site da Vice, junto com uma fotografia do entrevistador com o entrevistado e, escondido entre os *bits*, um "brinde": a geolocalização: McAfee estava na Guatemala[22].

Mas talvez o grande momento que atesta a fundamental importância dos metadados tenha sido a sua participação decisiva na identificação

21. FERRAN, Lee. **Ex-NSA Chief: 'We Kill People Based on Metadata'**. Disponível em: https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata. Acesso em: 21 fev. 2023.

22. WILHELM, John. **Vice leaves metadata in photo of John McAfee, pinpointing him to a location in Guatemala**. Disponível em: https://thenextweb.com/news/vice-leaves-metadata-in-photo-of-john-mcafee-pinpointing-him-to-a-location-in-guatemala. Acesso em: 8 jun. 2021.

do famoso *serial killer* americano BTK (acrônimo de "*Bind, Torture, Kill*" – "Amarrar, Torturar e Matar"), que aterrizou Wichita, Kansas desde 1974[23].

O criminoso possuía um *modus operandi* de observar e seguir as suas vítimas, surpreendê-las em suas casas e as amarrar. Tinha prazer sexual em vê-las morrendo sufocadas com um plástico na cabeça.

Narcisista, BTK gostava de se comunicar com os jornais, se gabando dos seus ataques.

Trinta anos após os primeiros assassinatos, em 2004, os jornais passaram a rememorar o terror causado pelo BTK, estimando que, tendo em vista que a última vítima foi em 1991, provavelmente o criminoso estivesse preso ou morto.

Irritado, BTK volta ao seu hábito de se comunicar com os jornais por meio de cartas, nas quais afirmava estar livre. Em uma das suas comunicações com os jornais, enviou uma mensagem em que perguntava: "*Posso me comunicar por um disquete e não ser rastreado até um computador? Sejam honestos*"[24]. A resposta, apresentada em uma mensagem em código publicada nos classificados de um jornal, declarava que não havia qualquer problema.

O *serial killer* cumpre a sua promessa, e o jornal recebe um disquete de 3.5 polegadas. Dentro, apenas um arquivo de texto, intitulado "TestA.rtf"[25]. O mais importante não eram os dados, mas os seus metadados. Ao analisar as suas propriedades, verificou-se que o autor do documento era um "Dennis", e que o proprietário do computador de onde saiu o texto era a Igreja Luterana de Cristo.

Uma simples pesquisa pelo Google foi suficiente para descobrir que o presidente da igreja era alguém que atendia por "Dennis Rader". A polícia obteve acesso ao exame de Papanicolau de Kerry, a filha de

23. SOUSA, Alana. **O que aconteceu com o assassino BTK?** Disponível em: https://aventurasnahistoria.uol.com.br/noticias/almanaque/o-que-aconteceu-com-o-assassino-btk.phtml. Acesso em: 9 jun. 2021.

24. VIGGIANO, Giuliana. **Quem é Dennis Rader, serial killer que se autodenominava "Assassino BTK**". Disponível em: bit.ly/3oYKSbR. Acesso em: 9 jun. 2021.

25. Os arquivos com extensão.RTF atendem ao formato *Rich Text Format*, criado pela Microsoft para permitir a portabilidade de documentos de texto entre diversos programas.

Dennis, e cruzou com a informação genética contida no sêmen que BTK deixou em uma cena de crime[26].

BTK, portanto, era Dennis Radder, um funcionário público tido como "rigoroso". Dennis foi condenado à 10 penas de prisão perpétua.

Em um mundo cercado por dados, não existe informação irrelevante.

d) Quanto à confidencialidade: há provas digitais *abertas*, que se referem àquelas em que não há restrições de segurança quanto o seu acesso, e as *criptografadas* ou *fechadas*, que dependem, para o conhecimento do seu conteúdo, do uso de senhas ou outras formas de autenticação. O investigado em inquérito ou o réu em ação penal não podem ser compelidos a entregar as senhas dos seus documentos e dispositivos digitais (computadores, *tablets* e *smartphone*s, por exemplo), sob pena de se ofender o princípio constitucional que veda a autoincriminação (art. 5º, LXIII, CF)[27].

1.4. Validade e força probante das provas documentais digitais

Segundo Marinoni e Arenhart, "(...) vê-se a carência efetiva de dispositivos para tratar da força probante do documento eletrônico, especificamente em razão da dificuldade em se ter por autêntica a informação transmitida por via digital"[28].

É importante chamar atenção que, muito embora a legislação costuma se referir à "documentos eletrônicos", é comum na doutrina

26. DOUGLAS, John; DODD, Johnny. **Inside the Mind of BTK**: the true story behind the thirty-year hunt for the notorious Wichita serial killer. São Francisco, EUA: John Wiley & Sons, Inc., 2007. p. 251-254.

27. "Habeas corpus. Medida cautelar inominada. Busca e apreensão de coisas. Investigação do paciente em crime de lavagem de dinheiro. Decisão fundamentada. Acesso aos aparelhos eletrônicos. Obrigatoriedade do réu em fornecer as senhas dos dispositivos eletrônicos. Impossibilidade. Postulado constitucional da não produção de provas contra si. Participação da ordem dos advogados do Brasil no feito. Incompatibilidade com o rito célere do habeas corpus. Aditamento da inicial. Impossibilidade após a instrução do writ. Limitação do objeto da investigação. Descoberta fortuita de crimes (serendipidade). Juridicamente impossível. Trata-se de resultado da investigação e não seu pressuposto ou condicionamento. Habeas corpus parcialmente concedido" (STJ – HC 580664 / RJ / HABEAS CORPUS – 2020/0111177-4 – Relator: Min. Ministro NEFI CORDEIRO – Data do Julgamento: 20/10/2020 – Data da Publicação/FonteDJe: 12/11/2020).

28. MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Prova e convicção.** 5. ed. São Paulo: Thomson Reuters, 2019. p. 660.

e na prática forense o emprego de "documentos digitais", razão pela qual tais conceitos serão tratados como sinônimos.

O art. 225 do Código Civil limita-se a declarar que diversas espécies de reproduções, dentre elas, as "eletrônicas", fazem prova plena dos fatos e das coisas que ostentam, desde que não haja impugnação quanto à exatidão, isto é, desde que essa cópia corresponda ao original.

Há no Código de Processo Civil algumas normas pontuais que tratam de documentos eletrônicos.

O art. 411 determina que o documento será "considerado autêntico" em 3 hipóteses, dentre elas, quando a autoria for identificada por processo de certificação, que poderá ser eletrônico (inciso II) e, quando não houver impugnação (III).

De acordo com o art. 422, *caput,* CPC, as reproduções (mecânicas ou de outra espécie) tem *aptidão* para fazer prova de fatos ou de coisas representadas, desde que não impugnadas, com redação muito semelhante ao já citado art. 225, CC.

O § 1º estabelece regramento semelhante às fotografias digitais ou "extraídas da internet", conduto, define um ônus à parte que a produziu em caso de eventual impugnação: a apresentação da "autenticação eletrônica", sem, contudo, explicar o que seria. Em não sendo possível comprovar a autenticação, seria necessária a realização de perícia.

A fotografia digital e a "extraída da Internet", anexada aos autos como prova documental, são apenas cópias de arquivos digitais originadas de uma câmera ou outro dispositivo capaz de fotografar ou de imagens registradas por terceiros e postadas na Internet.

Muito embora o CPC estabeleça o ônus processual de apresentação da autenticação só após a impugnação, nada impede que a parte apresente, simultaneamente, a prova e a sua respectiva autenticação.

Para a fotografia digital, a autenticação seriam os seus metadados, como, por exemplo, a indicação do dispositivo que fez o registro fotográfico (modelo da câmera), data e hora da criação etc. Já para a imagem extraída da Internet, a comprovação da sua origem (indicação da URL, por exemplo) e os seus respectivos metadados.

Determinou-se ainda a aplicação das regras do art. 422 à "forma impressa da mensagem eletrônica" (§ 3º). Aqui a autenticação