XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

LITON LANES PILAU SOBRINHO

RIVA SOBRADO DE FREITAS

JÉSSICA FACHIN

I61

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Liton Lanes Pilau Sobrinho, Riva Sobrado De Freitas, Jéssica Fachin – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-65-5274-079-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: UM OLHAR A PARTIR DA INOVAÇÃO E DAS NOVAS TECNOLOGIAS

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 2. Dinâmicas da segurança pública e internacional. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

O XXXI Encontro Nacional do CONPEDI ocorreu nos dias 27, 28 e 29 de novembo de 2024, em Brasília/DF. O evento teve como temática central "Um Olhas a partir da Inovação e das Novas Tecnologias".

As discussões realizadas durante o encontro, tanto nas diversas abordagens tecnológicas como nos Grupos de Trabalho (GTs), foram de grande relevância, considerando a atualidade e importância do tema.

Nesta publicação, os trabalhos apresentados como artigos no Grupo de Trabalho "Internet: Dinâmicas da Segurança Pública e Internacional I", no dia 29 de novembro de 2024, passaram por um processo de dupla avaliação cega realizada por doutores. A obra reúne os resultados de pesquisas desenvolvidas em diferentes Programas de Pós-Graduação em Direito, abordando uma parte significativa dos estudos produzidos no âmbito central do Grupo de Trabalho.

As temáticas abordadas refletem intensas e numerosas discussões que ocorrem em todo o Brasil. Elas indicam a urgência de pensar a tecnologia a partir dos direitos humanos, apontam para a problemática do discurso de ódio, indicando necessidade de educação para a cidadania digital, os desafios para a democracia frente à infodemia e ao contexto das fake news, bem como a definição desta e reflexões atuais e importantes sobre a regulação das plataformas digitais.

Esperamos que, por meio da leitura dos textos, o leitor possa participar dessas discussões e obter um entendimento mais amplo sobre o assunto. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e na organização do evento, cujas contribuições inestimáveis foram fundamentais, e desejamos uma leitura proveitosa!

Liton Lanes Pilau Sobrinho

(Universidade Federal de Santa Catarina)

Riva Sobrado de Freitas

(Universidade do Vale do Itajaí)

Danielle Jacon Ayres Pinto

(Universidade do Oeste de Santa Catarina)

Jéssica Fachin

(Universidade de Brasília e Faculdades Londrina)

A INTERNET DAS COISAS (IOT) E A PRODUÇÃO DE PROVAS: ADMISSIBILIDADE DOS DADOS COLETADOS PELOS DISPOSITIVOS ELETRÔNICOS NO PROCESSO CIVIL

THE INTERNET OF THINGS (IOT) AND EVIDENCE PRODUCTION: ADMISSIBILITY OF DATA COLLECTED BY ELECTRONIC DEVICES IN CIVIL PROCESS

Natalia Souza Machado Vicente
Diego Bianchi de Oliveira

Resumo

A revolução tecnológica proporcionada pela Internet das Coisas (IoT) tem transformado diversos aspectos da vida cotidiana, conectando dispositivos eletrônicos à internet e permitindo a coleta, troca e análise de dados em tempo real. No campo jurídico, essa inovação traz questões relevantes, especialmente sobre a admissibilidade dos dados coletados como provas no processo civil. A utilização de dados IoT em processos judiciais apresenta desafios e oportunidades. A coleta contínua de dados pode fornecer provas mais precisas e reduzir custos, mas a admissibilidade depende de autenticidade, integridade e confiabilidade dos dados. Além disso, a integração de dispositivos IoT levanta preocupações sobre privacidade e proteção de dados, conforme a Lei Geral de Proteção de Dados (LGPD), e desafios de interoperabilidade e segurança cibernética. A IoT oferece um vasto potencial para a produção de provas no processo civil, mas sua implementação requer uma abordagem cuidadosa para garantir a admissibilidade e confiabilidade dos dados. A adoção de tecnologias avançadas e a conformidade com regulamentações de proteção de dados são essenciais. A IoT pode modernizar o sistema judiciário, tornando-o mais ágil, preciso e econômico, mas é necessário adotar medidas robustas de segurança e validação por peritos para maximizar seus benefícios.

Palavras-chave: Internet das coisas (iot), Admissibilidade, Autenticidade, Privacidade, Segurança cibernética

Abstract/Resumen/Résumé

The technological revolution brought about by the Internet of Things (IoT) has transformed several aspects of everyday life, connecting electronic devices to the internet and allowing the collection, exchange and analysis of data in real time. In the legal field, this innovation raises relevant questions, especially regarding the admissibility of data collected as evidence in civil proceedings. The use of IoT data in legal proceedings presents challenges and opportunities. Continuous data collection can provide more accurate evidence and reduce costs, but admissibility depends on the authenticity, integrity, and reliability of the data. Furthermore, the integration of IoT devices raises concerns about privacy and data protection, according to the General Data Protection Law (LGPD), and interoperability and

cybersecurity challenges. IoT offers vast potential for producing evidence in civil proceedings, but its implementation requires a careful approach to ensure data admissibility and reliability. Adopting advanced technologies and complying with data protection regulations are essential. IoT can modernize the judicial system, making it more agile, accurate and economical, but it is necessary to adopt robust security measures and validation by experts to maximize its benefits.

Keywords/Palabras-claves/Mots-clés: Internet of things (iot), Admissibility, Authenticity, Privacy, Cybersecurity

Introdução

A revolução tecnológica proporcionada pela Internet das Coisas (IoT) tem transformado diversos aspectos da vida cotidiana, conectando dispositivos eletrônicos à Internet e permitindo a coleta, troca e análise de dados em tempo real. Desde eletrodomésticos inteligentes até sensores industriais, a IoT abrange uma vasta gama de dispositivos que monitoram e transmitem informações continuamente. No campo jurídico, essa inovação tecnológica traz à tona uma série de questões relevantes, especialmente no que diz respeito à admissibilidade dos dados coletados por esses dispositivos como provas no processo civil.

A utilização de dados provenientes de dispositivos IoT em processos judiciais apresenta tanto desafios quanto oportunidades. Por um lado, a coleta massiva e contínua de dados pode fornecer provas mais precisas e atualizadas, aumentando a eficiência na resolução de litígios e reduzindo os custos associados à coleta e análise de provas. Por outro lado, a admissibilidade desses dados depende de sua autenticidade, integridade e confiabilidade, critérios essenciais para garantir que as informações apresentadas sejam genuínas, não alteradas e precisas.

Além disso, a integração de dispositivos IoT no contexto jurídico levanta preocupações significativas relacionadas à privacidade e proteção de dados, especialmente à luz da Lei Geral de Proteção de Dados (LGPD). A diversidade de dispositivos e a falta de padrões uniformes também representam desafios para a interoperabilidade e a análise dos dados coletados. A segurança cibernética é outro aspecto crítico, uma vez que a vulnerabilidade dos dispositivos IoT a ataques pode comprometer a integridade e a confiabilidade das informações.

Este artigo jurídico visa explorar a interseção entre a IoT e a produção de provas no processo civil, analisando os critérios de admissibilidade dos dados coletados por dispositivos eletrônicos e discutindo as implicações de sua utilização no sistema judiciário.

Para tanto, valeu-se da aplicação do método dedutivo, que parte de considerações gerais para abordar um ponto específico. A pesquisa foi desenvolvida em nível exploratório e descritivo, procurando levantar informações e o detalhamento do objeto de estudo. Analisa-se, ainda, a legislação específica e a literatura especializada, lançando mão das técnicas de pesquisa bibliográfica.

O trabalho foi dividido em quatro seções. Inicialmente, é apresentado uma noção geral da Internet até a chegada da Internet das Coisas (IoT). Na sequência, verifica-se como a atividade probatória no processo civil pode ser valer-se dos dados coletados por

dispositivosIoT. A seguir,realizou-se uma análise dos conceitos de autenticidade, integridade e confiabilidade. E encerrou-se a pesquisa avaliando os desafios e oportunidades associados à IoT, buscando fornecer uma melhor compreensão das potencialidades e limitações dessa tecnologia no campo jurídico e, em especial, no processo civil.

1 Mas afinal, o que é Internet das Coisas (IoT)?

Sabe-se que a Internet – termo que advém da palavra *inter-network* – corresponde a uma rede de computadores interligados "mediante protocolos (IP, abreviação de *Internet Protocol*). Ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra ótica, satélites, ondas de rádio ou infravermelho" (Pinheiro, 2021, p. 40).

A Internet liga empresas, universidades, governose milhões de pessoas, independentemente de fronteiras geográficas.Acredita-se que se vive numadas maiores revoluções no campo da comunicação, em que indivíduos comuns descobrem habilidades e formas de expressão que dificilmente poderiam explorar nos meios tradicionais. Eles se tornam criadores, em diversos formatos, como fotografia, música, audiovisual, textos, hipertextos, conhecimento, cultura, educação, entretenimento, entre outros (Gobbi, 2011, p. 203).

Segundo a Pesquisa Nacional por Amostra de Domicílios 2023 (PNAD/2023), divulgada pelo Instituto Brasileiro de Geografia e Estatística - IBGE, entre os brasileiros com 10 anos ou mais de idade, a utilização da Internet subiu de 87,2%, em 2022, para 88,0%, em 2023, segundo dados coletados no período de referência da pesquisa. O percentual de usuários de Internet cresce a cada ano. Em 2016, ano em que o IBGE iniciou a série de pesquisas, o percentual de usuários era de 66,1% da população de 10 anos ou mais (IBGE, 2023).

Desde a abertura da Internet ao mercado comercial e sua consequente popularização, testemunha-se quase três décadas de profundas transformações estruturais e culturais. Manuel Castells (2005, p. 17)afirma que esse fenômeno representa um processo multidimensional, impulsionado pela ascensão de um novo paradigma tecnológico, cujas bases estão nas tecnologias de comunicação e informação. A Internet altera a dinâmica das relações sociais e econômicas, além de possibilitar uma maior integração global, conectando pessoas, empresas e instituições de maneira ubíqua.

A Internet e a tecnologia móvelpermitem que movimentos se tornem autoconscientes e identificáveis em tempo real. Da mesma forma como, individualmente, refletimos sobre suas atividades diárias e seus pensamentos via Twitter ou Facebook, compartilhando isso com a comunidade, a sociedade está passando por um processo constante de reflexividade e adaptação (Botsman; Rogers, 2011, p. 176).

Após conectar as pessoas, a Internet avança ao envolver também os objetos em sua teia virtual. Essa rede de hiperconectividade, com interações inteligentes entre pessoas, entre pessoas e objetos, e até entre os próprios objetos, é possibilitada pela chamada Internet das Coisas (IoT). Hoje, a IoT está sendo aplicada em várias áreas da sociedade, promovendo o desenvolvimento de cidades inteligentes, a automação de setores industriais (Indústria 4.0), a implementação da agricultura de precisão no meio rural e a melhoria da eficiência da administração pública.

A Internet das Coisas (*Internet ofThings*- IoT) é um "ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos", esse ambiente acaba por criar "um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia" (Magrani, 2018, p. 20).

O Decreto n. 9.854/19 – que trata do Plano Nacional de Internet das Coisas –, em seu art. 2º, inciso I, conceitua a IoT como "a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade".

Para ilustrar as potencialidades das IoT, imagine que ao chegar à sua casa, você acesse o seu *tablet* pessoal e procure a receita que você deseja fazer para o jantar; neste momento, seu *tablet* se conecta a geladeira, que informa se falta algum ingrediente. Caso alguém que more com você esteja em um supermercado, uma mensagem poderá ser enviada pela geladeira avisando da necessidade da compra do tal ingrediente faltante (Pasqualotto; Bublitz, 2017, p. 66). Outro exemplo, é a utilização de sistemas de automação residencial que "permitirão que um consumidor, antes mesmo de chegar à sua residência, possa enviar mensagem para que os próprios dispositivos realizem ações para abrir os portões, desligar alarmes, preparar o banho quente, colocar música ambiente e alterar a temperatura da casa" (Magrani, 2018, p. 24).

Não é equivocado dizer que a Internet das Coisas (IoT) "corresponde à fase atual da internet em que os objetos se relacionam com objetos humanos e animais os quais passam a

ser objetos portadores de dispositivos computacionais capazes de conexão e comunicação" (Santaella; et. al., 2013, p. 28).Esse avanço gera uma coleta e armazenamento massivo de dados, incluindo informações pessoais sobre a identidade, localização e preferências dos usuários.

Com o crescimento exponencial de dispositivos conectados à rede, a coleta de dados pela IoT atinge um nível sem precedentes. No entanto, essa proliferação de informações traz à tona questões importantes no campo jurídico, especialmente em relação à admissibilidade e validade desses dados como provas em processos judiciais. A interligação contínua de dispositivos e a capacidade de capturar dados em tempo real criam novos desafios e oportunidades para o processo civil, que devem ser analisados à luz da legislação e da proteção de direitos fundamentais.

2 A Internet das Coisas (IoT) e a Produção de Provas

Viu-se que a IoTse refereà interconexão de dispositivos físicos que, equipados com sensores e softwares, coletam e compartilham dados através da Internet. Essa rede inteligente abrange uma vasta gama de equipamentos, desde eletrodomésticos conectados, como geladeiras e televisores, até dispositivos complexos usados em ambientes industriais e urbanos, como sensores de tráfego, equipamentos médicos, e sistemas de automação residencial. Essa tecnologia permite a coleta e transmissão contínua de informações em tempo real, criando um fluxo constante de dados que pode ser aproveitado para diversas finalidades, incluindo o uso no campo jurídico (Bias, 2023).

No contexto do Direito Processual Civil, os dados gerados por dispositivos IoT têm o potencial de desempenhar um papel significativo como provas. Esses dados podem incluir registros de monitoramento de câmeras de segurança, informações de sensores de movimento em edifícios, dados de localização de veículos e registros de saúde coletados por dispositivos vestíveis, como *smartwatches*. O crescente uso desses dispositivos na vida cotidiana gera um vasto volume de informações que pode ser explorado em litígios civis para corroborar ou refutar alegações das partes envolvidas.

Antes de prosseguir, convém explicar que a prova é o meio que se permite persuadir alguém a respeito de algo, isto é, trata-se da demonstração da verdade de determinado fato.Em âmbito processual, conforme explica Alexandre Freitas Câmara (1999, p.339), a prova refere-se a qualquer elemento que contribui para formação da convicção do juiz a respeito da

existência de determinado fato, isto é, tudo aquilo que for levado aos autos com o fim de convencer o juiz de que determinado fato ocorreu será chamado de prova.

Na atividade cognitiva do processo, o juiz "tradicionalmente é visto como alguém que tem por função precípua a reconstrução dos fatos a ele narrados, aplicando sobre esses a regra jurídica abstrata contemplada pelo ordenamento positivo" (Marinoni; Mitidiero; Arenhart, 2015, p. 243).Sem dúvida, as "provas fornecem ao juiz os elementos necessários para a reconstrução, em juízo, de acontecimentos passados, com a finalidade de que ele possa formar o seu próprio convencimento sobre a verdade ou não dos fatos históricos alegados pelas partes" (Cambi, 2001, 49).

Embora o destinatário da prova seja o juiz, as provas são produzidas para o processo, não para um determinado magistrado. Considerando que o processo – incluindo inúmeras mudanças de juízes e a fase recursal – geralmente passa por mais de um julgador, é necessário que nos autos haja prova necessária para persuadir o órgão judicial competente para o julgamento(Cambi, 2001, 54).

Vale dizer que os que os meios de prova são os mecanismos através dos quais a prova é levada para o processo, ou seja, "são as técnicas desenvolvidas para se extrair prova de onde ela jorra (ou seja, da fonte). São fontes de prova as coisas, as pessoas e os fenômenos" (Didier Junior, 2015, p. 39). "São típicos (ou nominados) os meios de prova quando concebidos e disciplinados pela Lei, e atípicos (ou inominados) quando ausente previsão legal" (Medina, 2018, p. 647).

A princípio, pode-se crer que os dados gerados por dispositivos IoT são enquadrados como meios de prova atípicos, na medida em que não possuem uma regulamentação expressa no CPC. Nos entanto, os dispositivos IoT, ao capturar e transmitir informações em tempo real, geram registros digitais que, ao serem armazenados em um formato acessível e passível de verificação, constituem documentos digitais (ou documentos eletrônicos) que podem ser utilizados como prova.

Nesse sentido, Fábio Caldas de Araújo afirma que: "Toda e qualquer informação que possa ser armazenada e seja objeto de tráfego eletrônico pode ser utilizada como documento eletrônico". O Código de Processo Civil brasileiro, por sua vez, reconhece a validade de documentos eletrônicos nos termos de seu art. 439. Portanto, fala-se em atipicidade parcial da prova, pois como leciona José Miguel Garcia Medina (2018, p. 647) "[...] a atipicidade não decorre da ausência de previsão normativa da prova, mas da falta de previsão legal de procedimento tendente à realização da prova".

Para que esses dados, uma vez documentados, sejam aceitos como provas, é essencial que atendam aos requisitos de autenticidade, integridade e confiabilidade. A autenticidade garante que os dados são genuínos e não foram manipulados, podendo ser verificada através de certificação digital e logs de auditoria. A integridade assegura que as informações não sofreram alterações desde sua coleta até sua apresentação, utilizando técnicas como *hashing* e *blockchain* para criar registros imutáveis. A confiabilidade, por sua vez, refere-se à precisão e consistência dos dados, o que pode ser garantido por meio da calibração e manutenção dos dispositivos, além da validação por peritos (Silva, 2024).

Contudo, a aplicação de dados de dispositivos IoT no processo civil não está isenta de desafios. Um dos principais obstáculos está relacionado à proteção de dados e à privacidade dos indivíduos, especialmente em conformidade com a Lei Geral de Proteção de Dados (LGPD). Considerando que muitos desses dispositivos coletam dados sensíveis, como informações de localização, comportamento de consumo e até mesmo dados biométricos, é fundamental que os princípios de transparência, segurança e minimização de dados sejam rigorosamente observados, de modo a evitar o uso abusivo ou indevido dessas informações. A falta de regulamentações uniformes e de padrões técnicos claros para os dispositivos IoT pode gerar complicações adicionais, dificultando a interoperabilidade entre sistemas distintos e a análise dos dados.

Outro desafio relevante está relacionado à segurança cibernética. A vulnerabilidade dos dispositivos IoT a ataques cibernéticos pode comprometer a integridade dos dados coletados, expondo os sistemas a invasões que visam alterar ou corromper as informações, o que representaria um risco significativo à sua validade como prova judicial. O uso de protocolos de segurança robustos, como firewalls avançados e redes seguras, é indispensável para mitigar esses riscos e garantir que os dados mantidos pelos dispositivos permaneçam confiáveis e protegidos.

A Internet das Coisas oferece um imenso potencial para a produção de provas no processo civil, especialmente à medida que a tecnologia continua a se expandir e a se tornar uma parte cada vez mais integral do cotidiano. No entanto, a implementação desse recurso no campo jurídico exige uma abordagem cautelosa, que deve equilibrar o uso dessas inovações com a observância rigorosa dos critérios legais e técnicos necessários para garantir que os dados coletados sejam admissíveis e confiáveis. Além disso, a conformidade com as regulamentações de proteção de dados, como a LGPD, e o investimento em segurança cibernética são componentes essenciais para que a IoT possa oferecer todos os seus benefícios no âmbito judicial.

3Admissibilidade dos Dados Coletados pelos Dispositivos IoT

No cenário atual, a admissibilidade dos dados coletados por dispositivos da Internet das Coisas (IoT) levanta questões importantes sobre a definição e aceitação de documentos eletrônicos como prova. O próprio conceito de documento não se limita mais aos formatos físicos ou manuscritos, mas inclui uma variedade de formas digitais que podem registrar e transmitir informações relevantes para o processo judicial.

Nesse sentido, Luiz Rodrigues Wambier e Eduardo Talamini (2013, p. 483) refletem que a concepção atual de documento deve abranger além daquilo que a ciência atualmente conhece, isto é, tudo o que possa vir a ser inventado capaz de conter a expressão de um pensamento. A holografia, a transmissão eletrônica de dados (via internet) também são documentos hábeis a demonstrar a ocorrência de fatos relevantes para o processo.

Entretanto, surge uma série de dúvidas quanto à origem e materialidade dos documentos produzidos em plataformas digitais, tendo em vista o receio de serem suscetíveis de manipulação, e, em consequência, possuir valoração diminuída ou desconsiderando-se seu critério-peso. No mesmo sentido, Cândido Rangel Dinamarco (2001, p. 07) lembra que à época do Código de Processo Civil de 1939 surgiram, igualmente, dúvidas quanto à validade e eficácia dos documentos elaborados através da máquina de escrever, já que houve o abandono dos documentos elaborados a próprio punho.

O Código de Processo Civil "trata dos documentos eletrônicos de forma bastante sucinta e evasiva, tanto que se recomenda a verificação da legislação própria a respeito, que atualmente é a Lei n. 11.419/06" (Hartmann, 2015, p. 815). Apesar da legislação dispor que os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário serão considerados originais para todos os efeitos legais (art. 11), ainda pairam muitas dúvidas acerca de sua segurança jurídica.

Para que o documento eletrônico tenha força juridicamente probante, "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" (Didier Junior, 2015, p. 2016). Entende-se, portanto, para que os dados coletados por dispositivos da Internet das Coisas (IoT) sejam considerados admissíveis, é fundamental que eles atendam aos requisitos de autenticidade, integridade e confiabilidade.

3.1 Autenticidade

No contexto dos dados gerados por dispositivos IoT, a autenticidade refere-se à capacidade de garantir que os dados são genuínos e que a origem é identificável. Diferentemente dos documentos tradicionais, onde a assinatura manuscrita pode atestar a autoria, a autenticidade dos dados digitais é frequentemente assegurada por mecanismos técnicos como assinaturas digitais e certificados eletrônico

Como bem destaca Antônio Terêncio Marques (2011, p. 133), a "autenticidade "implica a autoria identificável, a possibilidade de se identificar, com elevado grau de certeza, a autoria da manifestação de vontade representada no documento digital". No mesmo sentido, José Miguel Garcia Medina (2018, p. 667) afirma que: "Autenticidade é a certeza da proveniência ou autoria do documento".

Usualmente, a autoria de um documento tradicional, isto é, o que demonstra sua paternidade é a assinatura lançada no suporte físico; em se tratando de documento eletrônico, é a assinatura digital que tem a função de autenticação (Marques, 2011, p. 133). Logo, assinar algo em nada tem a ver com a forma, mas sim com o seu objetivo que é depositar um sinal, marca ou símbolo pessoal com o fim de dar-lhe segurança e confirmação.

Conforme dispõe o inciso II do art. 411 do Código de Processo Civil, haverá presunção de autenticidade quando "a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei". "Com isso, os documentos assinados digitalmente, passam a ter presunção de autenticidade e veracidade, não necessitando de sua autenticação por outros meios" (Alves, 2016).

A presunção, neste caso é relativa. Conforme alerta Fábio Caldas de Araújo (2023): "O acesso de uma pessoa à chave de assinatura digital de outra poderá provocar a emissão de documentos falsos. A prova desse uso indevido não será eletrônica, mas física, e com a possibilidade de prova testemunhal". O que reforça a ideia de que é necessário medidas de segurança tecnológicas adicionais para verificar a autenticidade dos dados digitais.

A validação por peritos é uma prática recomendada para assegurar a autenticidade dos dados IoT. Peritos podem analisar os dados e os métodos de coleta para confirmar que eles são confiáveis e não foram manipulados. Em alguns casos, pode ser necessário apresentar testemunhos de especialistas em tecnologia da informação para explicar a autenticidade dos dados ao tribunal.

3.2 Integridade

A integridade dos dados refere-se à garantia de que as informações não foram alteradas ou corrompidas desde sua coleta até sua apresentação como prova. No contexto dos dispositivos IoT, assegurar a integridade dos dados é importante para que eles sejam considerados confiáveis e admissíveis em processos judiciais(Augusto, 2023). Diversas técnicas podem ser empregadas para garantir essa integridade.

A forma mais comum de se garantir a integridade de dados digitais é uma antiga ferramenta: a criptografia – que atua embaralhando os dados, tornando-os incompreensíveis para qualquer pessoa que não tenha a chave adequada para descriptografá-los. Como Explica Sandro D'Amato Nogueira (2009, p. 28), trata-se de "um processo matemático para embaralhar uma mensagem digital, tornando sua leitura incompreensível por pessoas que não possuam a chave (código) para desembaralhar a mensagem".

O *software* que permite a utilização dessa técnica, confere a assinatura com a sequência de *bits* do documento digital, a fim de acusar a adulteração do mesmo, provando, desta sorte, a incongruência de informações entre a assinatura e o ciberdocumento. De modo que, o documento assinado eletronicamente por meio da criptografia assimétrica, será muito mais confiável que o documento tradicional ou físico (Marques, 2011, p. 140-141).

Os dispositivos IoT operam de forma distribuída, muitas vezes em ambientes vulneráveis a ataques cibernéticos. Sendo assim, a integridade dos dados pode ser verificada por meio de assinaturas digitais baseadas em criptografia assimétrica, onde a sequência de *bits* original do documento ou dado é comparada com a sequência assinada. Se houver qualquer divergência, a adulteração será detectada, invalidando a confiabilidade da prova.

De acordo com Augusto Tavares Rosa Marcacini(2006) o "[...] que se deve buscarpreservar é a sequência de *bits*, tal qual originalmente criada, não importando em que meio odocumento está gravado, ou se o meio é ou não alterável. E a criptografia assimétrica permite realizaresta tarefa, protegendo a integridade da sequência de *bits*".

Além da criptografia, novas tecnologias como o blockchain têm sido aplicadas para assegurar a integridade dos dados digitais, incluindo aqueles coletados por dispositivos IoT. O blockchain, como explica Tatiana Revoredo (2019)se trata de uma tecnologia de núcleo, que possibilita que grandes grupos de pessoas cheguem a um acordo e registrem transações permanentemente, sem uma autoridade central. A tecnologia recebe esse nome pois as transações são registradas em grupos conhecidos como blocos (*block*), e cada um desses blocos é criptograficamente "selado" ao bloco anterior, formando uma cadeia (*chain*).

A *blockchain* armazena suas informações de maneira similar a uma lista encadeada, com uma sequência contínua que começa a partir do bloco inicial. Cada bloco subsequente faz referência ao bloco anterior e inclui dados específicos, como transações e o *hash* próprio do bloco. Os *hashes* funcionam como funções matemáticas que convertem dados de entrada, como mensagens ou arquivos, em códigos alfanuméricos criptografados. Quando um novo bloco é criado, seu *hash* incorpora a assinatura do *hash* do bloco anterior, funcionando como um selo. Alterações em blocos anteriores podem invalidar o bloco afetado. Todos os *hashes* são registrados no livro razão e, uma vez registrados, não podem ser apagados (SOUZA, 2023, p. 22).

A combinação dessas tecnologias permite que os dados coletados por dispositivos IoT mantenham sua integridade desde a origem até o armazenamento final. Isso garante que os dados possam ser apresentados como prova em processos judiciais, com a confiança de que eles não foram manipulados ou adulterados.

Como afirma Daniel Drescher (2019, p. 154), a estrutura de dados *blockchain* é sensível a qualquer mudança, provocando um "ruído" enorme com a quebra das referências de *hash*. Além disso, a escrita ou reescrita da estrutura de dados demanda altos custos de processamento, desmotivando ações fraudulentas.

Sendo assim, pode-se afirmar que não há como alterar as informações depois de salvas. "Em sua essência, blockchain é uma tecnologia que grava transações de maneira que estas não possam ser apagadas depois, somente admitindo uma atualização sequencial, mantendo um histórico sem fim" (Castro, 2023, p. 244).

Enfim, assegurar a integridade dos dados coletados por dispositivos IoT é fundamental para sua admissibilidade em juízo. O uso de criptografia e blockchain oferece mecanismos eficazes para garantir que os dados sejam protegidos contra alterações indevidas, reforçando sua confiabilidade como prova.

3.3 Confiabilidade

A confiabilidade dos dados envolve a garantia de que as informações são precisas e foram coletadas de maneira consistente e confiável. No contexto dos dispositivos IoT, a confiabilidade é um aspecto importante, pois a precisão dos dados pode impactar diretamente a tomada de decisões e a validade das provas em processos judiciais(ANDERSEN, 2015).

Os dispositivos IoT, ao capturarem dados em tempo real de múltiplas fontes, precisam garantir que essas informações sejam coletadas e transmitidas de forma confiável.

Qualquer interferência, falha ou manipulação durante o processo de coleta, armazenamento ou transmissão pode comprometer a integridade dos dados, e, consequentemente, a sua admissibilidade como prova judicial. Por isso, o atual Código de Processo Civil dispõe que apenas serão admitidos documentos (ou dados) eletrônicos produzidos e conservados com a observância da legislação específica (art. 441) – em especial o art. 11 da Lei n. 11.419/06 e a Medida Provisória n. 2.200-1/2001.

No intuito de garantir os requisitos de "validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras, foi instituída a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil" (Medina, 2015, p. 438).

Viu-se que a assinatura digital permite a comprovação da autoria de um determinado conjunto de dados – qualquer informação coletada por dispositivo IoT – através de um código anexado ou logicamente associado a uma mensagem eletrônica.A verificação da origem do dado é feita com a chave pública do remetente – utiliza-se de uma base criptográfica de chaves. Nesse sentido, José Carlos de Araújo Almeida Filho (2015, p. 2014) leciona que "através de um sistema de codificação e, posteriormente decodificação, pelas denominadas chaves simétricas e assimétricas, se pode verificar a autenticidade da assinatura. Acaso não haja a decodificação de forma correta, o sistema identifica e o documento é rejeitado".

Diante da autenticação e confiabilidade de dados conferidas pela assinatura digital com a utilização de chaves públicas (criptografia assimétrica), verifica-se uma convergência a validade e eficácia probatória do conjunto de dados. Não obstante, no fito de garantir ainda mais credibilidade e no intuito de se evitar fraudes, criou-se o processo de certificação digital.

A certificação digital visa validar a propriedade de uma chave pública e é executada por uma entidade chamada Autoridade Certificadora, que é encarregada de emitir, renovar e revogar certificados digitais.Trata-se do reconhecimento do proprietário das chaves através de uma "terceira entidade de confiança dos interlocutores, que terá a incumbência de certificar a ligação entre a chave pública e a pessoa que emitiu, como também a sua validade" (Marques, 2011, p. 174)

Os certificados, dependendo do regulamento da respectiva Política de Segurança da sua Autoridade Certificadora, contêm dados do seu titular, como nome, números de documentos identificadores, entre outros. Ao tentar ilustrar, Sandro D'Amato Nogueira (2009, p. 39) compara o certificado digital a uma carteira de identidade virtual que permite a identificação segura de uma mensagem ou transação em rede de computadores por meio de

procedimentos lógicos e matemáticos para assegurar a confidencialidade, integridade das informações e confirmação de autoria.

No Brasil, a Autoridade Certificadora competente para estabelecer políticas de segurança é o Instituto Nacional de Tecnologia da Informação – ITI. De acordo com Fábio Caldas de Araújo (2016, p. 737) trata-se de uma autarquia federal que assume a responsabilidade pela guarda e conservação da integridade das Chaves Públicas do Brasil. O ITI é a autoridade certificadora raiz, ou seja, a autarquia será responsável por cadastrar as demais entidades que emitirão os certificados digitais.

O ITI é responsável por manter a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil –, cuja finalidade é regular autenticidade, integridade e validade jurídica de documentos em forma eletrônica. Instituída pela Medida Provisória n. 2.200-1/2001, a ICP-Brasil cuidou de designar o Comitê-Gestor de Políticas apto a fornecer os certificados eletrônicos, que irão assegurar a segurança e a confiabilidade dos documentos eletrônicos.

Assim, ao utilizar dispositivos IoT para a coleta de dados em um processo judicial, a confiabilidade desses dados é assegurada por uma série de mecanismos, como a criptografia e a certificação digital. No entanto, é importante ressaltar que, por mais avançada que seja a tecnologia, acredita-se que jamais se alcançará "a certeza inequívoca de confiabilidade, tanto no sistema eletrônico quanto no tradicional, ou em outro qualquer, mas, ainda assim, é possível imprimir uma confiabilidade necessária para a concretização de negócios jurídicos nesses meios" (Pinheiro, 2021, p. 265).

4Desafios e Oportunidades

A crescente adoção de dispositivos IoT (Internet das Coisas) traz consigo uma série de desafios que precisam ser enfrentados para garantir a eficácia e a segurança dessas tecnologias. Entre os principais desafios estão a privacidade e proteção de dados, a interoperabilidade entre diferentes dispositivos e a segurança cibernética. A coleta massiva de dados por dispositivos IoT levanta preocupações sobre a conformidade com a Lei Geral de Proteção de Dados (LGPD), enquanto a diversidade de dispositivos e a falta de padrões uniformes dificultam a integração e análise dos dados. Além disso, a vulnerabilidade dos dispositivos a ataques cibernéticos pode comprometer a integridade e a confiabilidade das informações coletadas (Barbosa, Ville, 2023)

Privacidade e Proteção de Dados: A coleta massiva de dados por dispositivos IoT levanta preocupações sobre a privacidade e a proteção de dados pessoais. A conformidade

com a Lei Geral de Proteção de Dados (LGPD) é essencial para garantir que os dados sejam coletados e utilizados de forma ética e legal. A falta de conformidade pode resultar em sérias penalidades e perda de confiança por parte dos usuários.

Interoperabilidade: A diversidade de dispositivos IoT e a falta de padrões uniformes podem dificultar a integração e a análise dos dados coletados. Sem interoperabilidade, os dispositivos podem não se comunicar de forma eficaz, resultando em sistemas fragmentados e ineficientes. A padronização é crucial para permitir a comunicação fluida entre diferentes dispositivos e plataformas.

Segurança Cibernética: A vulnerabilidade dos dispositivos IoT a ataques cibernéticos pode comprometer a integridade e a confiabilidade dos dados. Dispositivos inseguros podem ser alvos fáceis para hackers, que podem explorar essas vulnerabilidades para acessar informações sensíveis ou causar danos aos sistemas. Implementar medidas robustas de segurança cibernética é essencial para proteger os dados e garantir a confiança dos usuários.

Abordar esses desafios é fundamental para o sucesso e a sustentabilidade das soluções IoT, garantindo que elas possam ser utilizadas de forma segura, eficiente e em conformidade com as regulamentações vigentes.

Ademais, a integração de dispositivos IoT (Internet das Coisas) no campo jurídico apresenta uma série de oportunidades que podem transformar significativamente a maneira como os processos judiciais são conduzidos. A IoT oferece benefícios notáveis, como a eficiência na coleta de provas, a redução de custos e a promoção da inovação jurídica. Esses avanços tecnológicos têm o potencial de modernizar o sistema judiciário, tornando-o mais ágil, preciso e econômico. A seguir, exploraremos essas oportunidades em maior detalhe. (Silva, Silva, 2022)

Eficiência na Coleta de Provas: A IoT permite a coleta de dados em tempo real, proporcionando provas mais precisas e atualizadas. Sensores e dispositivos conectados podem registrar eventos e condições de maneira contínua, eliminando a necessidade de intervenções humanas e reduzindo a possibilidade de erros ou manipulações. Isso é particularmente útil em casos que envolvem monitoramento ambiental, vigilância de segurança e rastreamento de ativos.

Redução de Custos: A utilização de dispositivos IoT pode reduzir os custos associados à coleta e análise de provas. A automação de processos, como a captura de dados e a geração de relatórios, diminui a necessidade de mão de obra intensiva e reduz o tempo gasto em tarefas administrativas. Além disso, a IoT pode minimizar os custos de deslocamento e logística, uma vez que os dados podem ser acessados remotamente.

Inovação Jurídica: A adoção de tecnologias IoT no campo jurídico pode promover a inovação e a modernização dos processos judiciais. Ferramentas baseadas em IoT podem facilitar a gestão de casos, melhorar a comunicação entre as partes envolvidas e aumentar a transparência dos procedimentos. Por exemplo, tribunais podem utilizar dispositivos IoT para monitorar o cumprimento de medidas cautelares, como tornozeleiras eletrônicas, garantindo maior controle e segurança.

A incorporação de dispositivos IoT no sistema jurídico não só aprimora a eficiência e a precisão na coleta de provas, mas também oferece uma oportunidade para reduzir custos e fomentar a inovação. Esses avanços tecnológicos têm o potencial de revolucionar o campo jurídico, tornando os processos mais dinâmicos e acessíveis. À medida que a IoT continua a evoluir, é essencial que o setor jurídico acompanhe essas mudanças, adotando novas tecnologias de forma estratégica e ética para maximizar seus benefícios.

Considerações finais

O uso crescente e massivo de de dispositivos IoT (Internet das Coisas) na coleta de dados e sua introdução no campo jurídico como fonte de prova levanta algumas questõesrelacionadasa admissibilidade dessas informações.Conforme identificou-se, a admissibilidade dos dados coletados por dispositivos IoT depende da observância da legislação, especialmente o Código de Processo Civil e a Medida Provisória n. 2.200-1/2001, que estabelece a infraestrutura necessária para validar a produção e preservação de provas digitais.

O simples levantamento desses dados não é suficiente, é preciso garantir sua autenticidade, ou seja, assegurar que os dados realmente emanam da fonte que se alega. O Código de Processo Civil estabelece presunção de autenticidade quando a autoria estiver identificada por qualquer outro meio legal de certificação.

No que tange à integridade, identificou-se que a garantia de que os dados não foram alterados ou corrompidos durante sua transmissão e armazenamento é fundamental para sua aceitação como prova. Técnicas como criptografia e a emergente tecnologia *blockchain* oferecem soluções para assegurar a integridade, permitindo que as sequências de *bits* permaneçam inalteradas e imutáveis após sua criação. O uso de criptografia e a tecnologia blockchain aumentam a resistência a fraudes e garantem um registro confiável de transações e dados.

A confiabilidade, por sua vez, está intimamente ligada à autenticidade e precisão das informações coletadas. A certificação digital, regulada no Brasil pela ICP-Brasil, desempenha um papel central nesse quesito, permitindo a verificação da origem dos dados e assegurando sua validade jurídica. Embora o uso de chaves públicas e privadas proporcione um nível elevado de confiança, é importante reconhecer que a confiabilidade absoluta é inatingível, seja no sistema eletrônico ou no tradicional. No entanto, como destaca a doutrina, os mecanismos atuais oferecem uma confiabilidade suficiente para gerar presunção de segurança quanto a autenticidade e integridade dos dados.

Diante de todas essas considerações, a utilização de dados coletados por dispositivos IoT na atividade probatória no Processo Civil brasileiro passa pelo fortalecimento das infraestruturas de segurança, como a certificação digital, e pela adoção crescente de novas tecnologias, como *blockchain*, para preservar a integridade dos dados. Ao mesmo tempo, é necessário que os operadores do direito desenvolvam um conhecimento técnico adequado para avaliar a confiabilidade dessas provas e que o ordenamento jurídico continue a evoluir para acompanhar as inovações tecnológicas, assegurando que os direitos fundamentais das partes sejam resguardados. Dessa forma, enquanto essas tecnologias oferecem soluções promissoras, a cautela e a contínua revisão legislativa são fundamentais para garantir uma aplicação justa e eficiente.

REFERÊNCIAS

ALMEIDA FILHO, José Carlos de Araújo. **Processo eletrônico e teoria geral do processo eletrônico**: a informatização judicial no Brasil. 5. ed. Rio de Janeiro: Forense, 2015.

ALVES, Marcella Bizotto. As provas eletrônicas no novo CPC associadas ao advento do Marco Civil da Internet. **Migalhas**, 2016. Disponível em: https://www.migalhas.com.br/depeso/247105/as-provas-eletronicas-no-novo-cpc-associadas-ao-advento-do-marco-civil-da-internet. Acesso em: 06 ago. 2024.

ANDERSEN, Jason. O que a Confiabilidade tem a ver com a Internet das Coisas? **Stratus Blog**, 2015. Disponível em: https://blog.stratus.com/br/reliability-the-internet-of-things/. Acesso em: 13 ago. 2024.

ARAÚJO, Fábio Caldas de. **Curso de Processo Civil**. São Paulo: Revista dos Tribunais, 2023.

ARAÚJO, Fábio Caldas de. **Curso de direito processual civil**: parte geral. São Paulo: Malheiros, 2016.

AUGUSTO, Flávia. Desafios IoT: como a Internet das Coisas afeta a cibersegurança. **ManageEngine Blog**, 2023. Acesso em:https://blogs.manageengine.com/portugues/2023/12/30/desafios-iot-como-a-internet-das-coisas-afeta-a-ciberseguranca.html.Acesso em: 13 ago. 2024.

BARBOSA, Bruna Gavron. VALLE, Vivian Cristina Lima Lopez. Os desafios quanto a preservação da privacidade e da proteção de dados em face dos equipamentos IoT. **International Journal of Digital Law**, Belo Horizonte, v. 4, n. 1, p. 35-61, jan./abr. 2023

BIAS, Hebert Resende. A internet das coisas e o Direito: uma perspectiva pessoal.**Migalhas**, 2023. Disponível em: https://www.migalhas.com.br/depeso/395525/a-internet-das-coisas-e-o-direito-uma-perspectiva-pessoal.Acesso em: 05 ago. 2024.

BOTSMAN, Rachel; ROGERS, Roo. **O que é meu é seu**: como o consumo colaborativo vai mudar o nosso mundo. Tradução: Rodrigo Sardenberg. Porto Alegre: Bookman, 2011.

CÂMARA, Alexandre Freitas. **Lições de direito processual civil**. 2. ed. Rio de Janeiro: Lúmen Juris, 1999.

CAMBI, Eduardo. **Direito constitucional à prova no processo civil**. São Paulo: Revista dos Tribunais, 2001.

CASTRO, Manuella Santos de. Blockchain e Direitos Autorais. *In*: SILVA, Alexandre Pacheco; GUIMARÃES, Tatiane; MOUTINHO, Andréa Lesevicius. **Direito Autoral e Internet:** diagnósticos e perspectivas do debate brasileiro. São Paulo: Almedina, 2023.

DIDIER JUNIOR, Fredie; *et. al*. **Curso de direito processual civil:** teoria da prova, direito probatório, ações probatórias, decisão, precedente, coisa julgada e antecipação dos efeitos da tutela. v. 2. 10. ed. Salvador: JusPodivm, 2015.

DINAMARCO, Cândido Rangel. **Instituições de direito processual civil**. v. III. São Paulo: Malheiros, 2001.

DRESCHER, Daniel. **Blockchain Básico**: uma introdução não técnica em 25 passos. Tradução: Lúcia A. Kinoshita. São Paulo: Novatec, 2018.

GOBBI, Maria Cristina. A pesquisa empírica na sociedade digital. In: BARBOSA, Marialva; MORAIS, Osvando J. de. (org.). **Quem tem medo da pesquisa empírica?** São Paulo: Intercom, 2011.

HARTMANN, Rodolfo Kronemberg. **Curso completo de processo civil**. 2. ed. Rio de Janeiro: Impetus, 2015.

IBGE. **Pesquisa Nacional por Amostra de Domicílios Contínua 2023**. Disponível em: https://painel.ibge.gov.br/pnadc/. Acesso em: 11.08.2024.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV, 2018.

MARCACINI, Augusto Tavares Rosa. **O documentoeletrônico como meio de prova**. Disponível

em:http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico. Acesso em: 05 ago. 2024.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco; ARENHART, Sérgio Cruz. **Novo curso de processo civil**: tutela dos direitos mediante procedimento comum. v.2. São Paulo: Revista dos Tribunais, 2015.

MARQUES, Antônio Terêncio G. L. **A prova documental na internet:** validade e eficácia do documento eletrônico. Curitiba: Juruá, 2011.

MEDINA, José Miguel Garcia. **Curso de Direito Processual Civil Moderno**. 4. ed. São Paulo: Revista dos Tribunais, 2018.

MEDINA, José Miguel Garcia. **Novo código de processo civil comentado**: com remissões e notas comparativas ao CPC/1973. São Paulo: Revista dos Tribunais, 2015.

NOGUEIRA, Sandro D'amato. **Manual de direito eletrônico**. Leme: BH, 2009.

PASQUALOTTO, Adalberto de Souza; BUBLITZ, Michelle Dias. Desafios do presente e do futuro para as relações de consumo ante Indústria 4.0 e a Economia Colaborativa**. Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo**, v. 3, n. 2, p. 62-81, jul./dez. 2017.

PINHEIRO, Patricia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva, 2021.

SANTAELLA, Lucia; et. al. Desvelando a Internet das Coisas. **Revista GEMInIS**, v. 4, n. 2, p. 19-32, dez. 2013.

SILVA, Mikchaell Bastos Policarpo da. A eficácia e validade da prova digital no processo judicial brasileiro. **Jusbrsil**, 2024. Disponível em: https://www.jusbrasil.com.br/artigos/a-eficacia-e-validade-da-prova-digital-no-processo-judicial-brasileiro/2490635874#_ftn1. Acesso em: 05 ago. 2024.

SILVA, Thiago Mamede Menezes Silva. SILVA, Diogo Severino Ramos da. Inteligência Artificial à luz do Direito: Integração na sociedade e meios de regulamentação. **Jusbrasil**, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/inteligencia-artificial-a-luz-do-direito-integracao-na-sociedade-e-meios-de-regulamentacao/1720573976. Acesso em: 07 ago. 2024.

SOUZA, Gustavo Toledo de. **Aplicação da Tecnologia Blockchain na autenticidade de documentos**. 2023. 75 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) – Pontifícia Universidade Católica de Goiás, Goiânia, 2023.

WAMBIER, Luiz Rodrigues; TALAMINI, Eduardo. **Curso avançado de processo civil**: teoria geral do processo e processo do conhecimento. v. 1. 13. ed. São Paulo: Revista dos Tribunais, 2013.