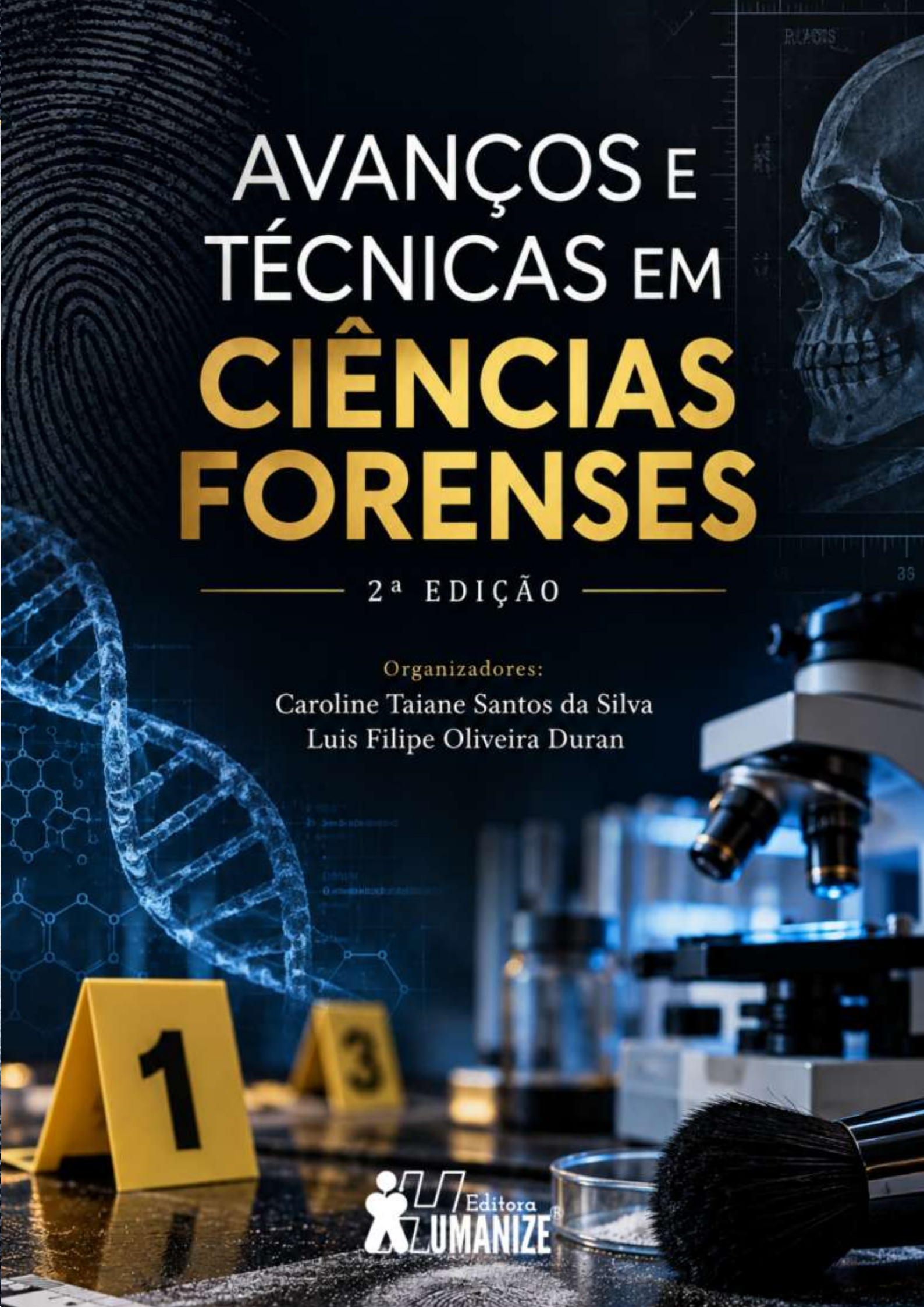




# AVANÇOS E TÉCNICAS EM CIÊNCIAS FORENSES

— 2ª EDIÇÃO —

Organizadores:

Caroline Taiane Santos da Silva  
Luis Filipe Oliveira Duran

Avanços e Técnicas em Ciências Forenses

**ORGANIZADORES**  
Caroline Taiane Santos da Silva  
Luis Filipe Oliveira Duran

AVANÇOS E TÉCNICAS EM CIÊNCIAS FORENSES



Copyright © Editora Humanize

Todos os direitos reservados

A reprodução não autorizada desta publicação, no todo ou em parte, constitui violação do copyright (Lei 5.988/73 e Lei 9.61/98)

Texto revisado segundo o novo Acordo Ortográfico da Língua Portuguesa

Direito de publicação concedida a Editora Humanize

### **Organização**

Luis Filipe Oliveira Duran

Caroline Taiane Santos da Silva

### **Editora Responsável**

Editora Humanize

### **Revisão Editorial, Normalização e Catalogação**

Equipe Técnica da Editora Humanize

### **Projeto Gráfico e Diagramação**

Equipe de Design Editorial da Editora Humanize

### **Publicação**

Editora Humanize

#### **Dados Internacionais de Catalogação na Publicação (Editora Humanize, BA, Salvador)**

A946t  
AF88526 SILVA, Caroline Taiane Santos da; DURAN, Luis Filipe Oliveira.

Avanços e Técnicas em Ciências Forenses – Bahia / BA: Editora Humanize, 2026  
1 Livro digital; ed. II; il.

ISBN: 978-65-5255-230-3

CDD 363.25

CDU 343.98

1. Alfabetização. 2. Letramento. 3. Contação de histórias. 4. Práticas pedagógicas. 5. Anos iniciais do Ensino Fundamental.

---

1. Investigação criminal e ciências forenses - CDD: 363.25

2. Criminalística- CDU: 343.98

# APRESENTAÇÃO DA OBRA

As ciências forenses desempenham um papel fundamental na investigação científica, na produção de provas e no fortalecimento da justiça. Em um cenário de constantes transformações tecnológicas e metodológicas, a atualização do conhecimento e o compartilhamento de experiências tornam-se essenciais para o aprimoramento das práticas periciais e o desenvolvimento de novas abordagens investigativas.

A obra “**Avanços e Técnicas em Ciências Forenses – 2ª Edição**” surge com o propósito de reunir pesquisas, estudos e experiências que contribuam para a ampliação do conhecimento científico nas diferentes áreas da perícia e da investigação forense. Por meio de uma abordagem multidisciplinar, a publicação contempla avanços tecnológicos, metodologias analíticas, desafios contemporâneos e aplicações práticas relacionadas às ciências forenses.

Estruturada na modalidade de **publicação em fluxo contínuo**, esta edição permite a incorporação progressiva de novos capítulos, proporcionando uma construção coletiva e dinâmica do conhecimento. Dessa forma, a obra permanece aberta a diferentes temáticas, perspectivas e contribuições científicas, acompanhando a evolução das pesquisas e das demandas profissionais do campo forense.

Entre os assuntos inicialmente abordados, destacam-se a utilização de dispositivos vestíveis e tecnologias da Internet das Coisas (IoT) na perícia digital, bem como os desafios relacionados à diversificação de produtos contendo substâncias psicoativas e sua análise laboratorial. Essas discussões representam apenas parte das possibilidades temáticas que serão ampliadas com a inclusão de novos estudos ao longo da publicação.

Destinada a estudantes, pesquisadores, docentes, peritos criminais e profissionais de áreas correlatas, esta obra busca estimular o pensamento crítico, a interdisciplinaridade, o rigor metodológico e a aplicação responsável do conhecimento científico.

Agradecemos aos autores que contribuem para esta edição e reafirmamos nosso compromisso com a valorização da pesquisa, a disseminação do conhecimento e o fortalecimento das ciências forenses.

Esperamos que esta publicação constitua uma fonte relevante de consulta, reflexão e atualização profissional, incentivando novas investigações e contribuindo para o avanço contínuo da ciência e da justiça.



# SUMÁRIO

## **CAPÍTULO 01: TESTEMUNHAS INVISÍVEIS”: DISPOSITIVOS VESTÍVEIS E IOT NO CAMPO DA PERÍCIA DIGITAL..... 6**

|                              |    |
|------------------------------|----|
| Introdução .....             | 7  |
| Objetivo.....                | 10 |
| Metodologia .....            | 10 |
| Resultados e discussão ..... | 10 |
| Considerações finais.....    | 19 |
| Referências .....            | 21 |

## **CAPÍTULO 02: DIVERSIFICAÇÃO NAS FORMAS DE APRESENTAÇÃO DE PRODUTOS CONTENDO THC: EXPERIÊNCIA DO LABORATÓRIO DE NARCÓTICOS DA POLÍCIA CIENTÍFICA DE GOIÁS ..... 23**

|                              |    |
|------------------------------|----|
| Introdução .....             | 24 |
| Objetivo.....                | 25 |
| Metodologia .....            | 25 |
| Resultados e discussão ..... | 26 |
| Considerações finais.....    | 31 |
| Referências .....            | 31 |



CAPÍTULO

# 01

## **“TESTEMUNHAS INVISÍVEIS”: DISPOSITIVOS VESTÍVEIS E IoT NO CAMPO DA PERÍCIA DIGITAL**

AUTORIA

### **Maiara Marins Guimarães**

Pós-Graduada em Direito Penal e Processo Penal pela Universidade Cândido Mendes do Rio de Janeiro, Perita Judicial em Documentoscopia e Grafoscopia e Pós-Graduada em Perícia em Imagens e Documentos Digitais pela IPOG.

PERÍCIA DIGITAL / DISPOSITIVOS INTELIGENTES



## “TESTEMUNHAS INVISÍVEIS”: DISPOSITIVOS VESTÍVEIS E IOT NO CAMPO DA PERÍCIA DIGITAL

**Resumo:** O avanço contínuo das tecnologias digitais e a difusão da Internet das Coisas (IoT) transformaram radicalmente a maneira como a perícia forense interage com o ambiente ao seu redor. Atualmente, dispositivos inteligentes, sensores e wearables capturam o cotidiano de maneira quase imperceptível, tornando-se fontes de informação essenciais, “testemunhas invisíveis” dos eventos e contextos. Os dispositivos conectados passaram a registrar informações de forma contínua e autônoma, criando novas frentes de investigação, mas também impondo dilemas relacionados à metodologia, ao enquadramento jurídico e à conduta ética do perito. A multiplicidade de fabricantes, formatos de dados e padrões técnicos dificulta a criação de procedimentos uniformes, obrigando o especialista a adaptar sua atuação a ecossistemas heterogêneos. Além disso, a natureza efêmera e fragmentada das informações torna o processo de coleta e salvaguarda mais complexo, exigindo do perito uma abordagem ainda mais rigorosa. Não é suficiente apenas validar tecnicamente uma evidência: é crucial que sua coleta e análise estejam em conformidade com as normas legais que garantem sua admissibilidade em tribunal. Nesse cenário, é essencial ressaltar a importância das legislações que garantem a proteção de dados, como a Lei Geral de Proteção de Dados e o Regulamento Geral de Proteção de Dados da União Europeia. Essas normas sublinham a exigência de autorização judicial ou de consentimento explícito para que se possa acessar informações pessoais. Ademais, a manutenção cuidadosa da cadeia de custódia e a documentação detalhada de cada etapa da perícia são cruciais para garantir a integridade das evidências digitais. O perito desempenha o papel de intermediário entre esses diferentes contextos, sendo capaz de transformar dados técnicos em informações que são compreensíveis e confiáveis. Assim, o conceito das “testemunhas invisíveis” deixa de ser apenas um desafio e se torna uma nova possibilidade de fortalecer a justiça digital e a credibilidade na ciência forense.

**Palavras-chave:** Tecnologia; Internet das Coisas; Perícia Digital; Análise Forense; Cadeia de Custódia.

## INTRODUÇÃO

Ninguém pode contestar a influência profunda que a Internet das Coisas exerce sobre a vida cotidiana. Atualmente, essa tecnologia se manifesta em áreas essenciais, como saúde, transporte e eficiência energética, enquanto também influencia nosso entretenimento, qualidade de vida, aprendizado e até a vigilância do meio ambiente. Este é um processo de mudança que se desenrola simultaneamente em diversos contextos. Recentemente, temos observado um aumento significativo na criação de aplicativos, dispositivos e

assistentes virtuais que possibilitam o controle e a supervisão remota de diversos aparelhos, particularmente em lares conectados.

A IoT funciona por meio de uma infraestrutura composta por sensores, plataformas de comunicação e serviços remotos, todos organizados em camadas. Para que esse ecossistema opere sem interrupções, é necessário que protocolos e dispositivos de intermediação façam a tradução entre essas camadas, garantindo que os dados circulem de forma compreensível entre sistemas diferentes. Eles estabelecem as divisões entre as diferentes camadas e também asseguram que o sistema se comunique adequadamente.

É neste momento que a importância da análise forense digital se evidencia. Com o aumento do uso de dispositivos sensoriais em lares, dos relógios inteligentes que empregamos e dos sistemas automatizados, a dinâmica das investigações sofreu uma transformação. O trabalho pericial, que sempre foi fundamental para revelar a verdade técnica em investigações, agora precisa lidar com essas novas fontes de informação.

Esses dispositivos, frequentemente quase imperceptíveis em nossas rotinas diárias, são frequentemente chamados de "testemunhas invisíveis". Eles realizam um monitoramento contínuo de dados essenciais relacionados ao clima, à localização, aos nossos comportamentos e ao ambiente ao nosso redor. A rastreabilidade completa da evidência torna-se indispensável nesses cenários. Cada etapa, desde a obtenção dos dados até sua apresentação em juízo, precisa ser documentada para demonstrar que o material analisado permaneceu íntegro e confiável ao longo de todo o processo. Contudo, a expansão do universo digital levanta desafios significativos nos aspectos técnicos, legais e éticos para a investigação digital.

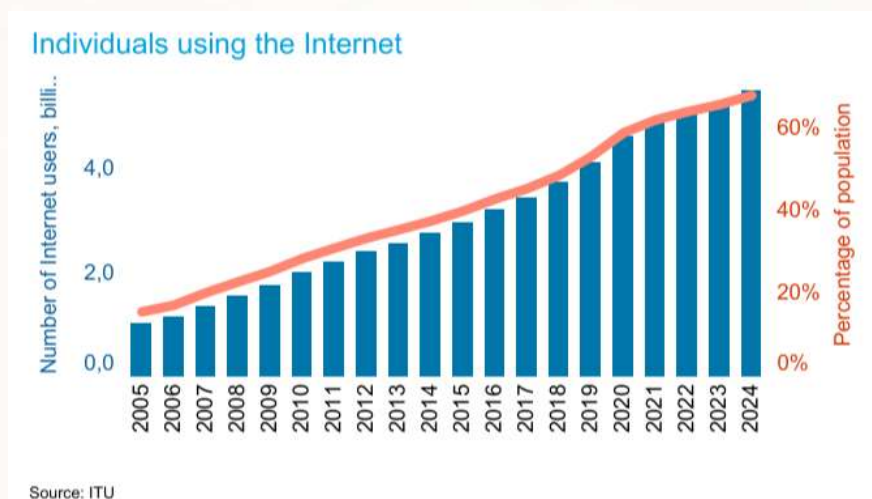
A instabilidade das informações, a diversidade das plataformas e a falta de normas entre os aparelhos de IoT tornam a obtenção e a manutenção de provas de uma forma que seja legitimamente aceita em termos periciais mais desafiadora. Além disso, os dispositivos de IoT frequentemente aplicam métodos sofisticados de criptografia e segurança com o intuito de proteger a privacidade e os dados dos usuários. Apesar de essas medidas de segurança serem essenciais para proteger informações delicadas, elas também criam barreiras significativas para os investigadores forenses, que precisariam decifrar e analisar os dados para coletar evidências relevantes.

Sob a perspectiva legal, surgem questões complicadas relacionadas à administração de dados pessoais, à privacidade e ao consentimento, exigindo uma interação entre legislações, princípios de segurança cibernética e boas práticas de investigação forense.

Assim, a atividade do especialista em perícia digital forense demanda muito além da mera competência técnica. É essencial também ter senso ético e entender a estrutura legal que rege a evidência. Apenas com essa harmonia entre saber tecnológico e dever legal é que se pode garantir que a obtenção e a avaliação das provas digitais sejam realizadas em respeito aos direitos fundamentais e satisfaçam as exigências necessárias para sua aceitação no sistema judiciário.

O crescimento da conectividade ao redor do mundo é inegável. De acordo com um estudo realizado pela União Internacional de Telecomunicações (UIT), que é a agência da ONU encarregada de supervisionar e padronizar as redes e serviços de telecomunicações globalmente, revelaram que 67% da população do planeta já faz uso de plataformas digitais, evidenciando uma tendência que apresenta previsões de expansão constante:

**Figura 1** - Individuals using the Internet



**Fonte:** ITU, 2024.

O contexto atual de hiperconexão tem promovido, de maneira quase inevitável, o rápido crescimento da Internet das Coisas (IoT). A multiplicação de dispositivos interligados altera o dia a dia e aumenta não somente a quantidade de usuários conectados, mas também a variedade de equipamentos aptos a captar ações, hábitos e condutas humanas. Cada novo aparelho adicionado a esse sistema traz novas informações, gerando um vasto e disperso conjunto de provas digitais, presente em todos os lugares, mas em algumas ocasiões complicado de gerenciar e compreender.

Diante dessa realidade, é fundamental entender mais a fundo a função que a Internet das Coisas e os dispositivos vestíveis desempenham na criação e confirmação de evidências digitais. Essa conversa vai além do aspecto técnico: abrange também questões éticas, legais e sociais, pois a mesma tecnologia que pode ajudar na busca pela verdade processual pode também ameaçar direitos essenciais, como a privacidade e a segurança dos dados.

Este estudo se propõe a discutir essas questões ao examinar os principais obstáculos que a perícia digital enfrenta em um mundo cada vez mais conectado. Os desafios vão além da simples coleta ou preservação de dados, estendendo-se à forma como essas provas são validadas e apresentadas de acordo com os requisitos legais.

Ao salientar aspectos como geolocalização, metadados, endereços IP, valores de hash e sincronização temporal, busca-se demonstrar como cada um desses detalhes técnicos pode impactar a confiabilidade da prova digital. Além disso, busca-se destacar a

necessidade urgente de políticas, protocolos e práticas forenses que garantam a veracidade e a aceitação desses registros, transformando as chamadas "testemunhas invisíveis" do ambiente digital em apoiadores legítimos da verdade científica e judicial.

## **OBJETIVO**

---

Realizar uma análise detalhada dos principais obstáculos que a perícia digital encontra em ambientes que utilizam a Internet das Coisas, levando em consideração as dimensões técnicas, legais e éticas envolvidas. Examinar as dificuldades associadas à coleta, preservação e manutenção da integridade dos dados gerados por dispositivos conectados, com foco em questões como volatilidade, interoperabilidade e limitações nos sistemas de armazenamento. Abordar os desafios técnicos e legais que cercam a admissibilidade e a validade das evidências digitais provenientes de dispositivos vestíveis e IoT, salientando a relevância de elementos como geolocalização, metadados, endereços IP, valores hash e sincronização temporal para a formulação e verificação da prova digital. Por último, a pesquisa busca avaliar as abordagens metodológicas e as novas tecnologias desenvolvidas para superar esses impedimentos, com o objetivo de reforçar a validade da prova digital no âmbito forense.

## **METODOLOGIA**

---

A presente pesquisa caracteriza-se como um estudo de caráter qualitativo, com delineamento exploratório-descritivo, fundamentada em revisão bibliográfica e documental. O objetivo da investigação é entender os desafios técnicos, legais e éticos relacionados à perícia digital no contexto da Internet das Coisas (IoT). Para isso, foram analisadas legislações, normas e publicações científicas relevantes. Também foram considerados padrões e melhores práticas internacionais, com destaque para a ISO/IEC 27037, que orienta os processos de identificação e preservação de evidências digitais. Além disso, relatórios e diretrizes de instituições reconhecidas, como o National Institute of Standards and Technology (NIST) e a International Telecommunication Union (ITU), foram utilizados. Essa metodologia possibilitou a formação de uma base teórica sólida, essencial para realizar uma análise crítica a respeito da aceitação e da integridade das provas digitais no contexto forense atual.

## **RESULTADOS E DISCUSSÃO**

---

### **Desafios da perícia digital em ambientes de IoT**

A análise digital em contextos de Internet das Coisas (IoT) enfrenta um ambiente cada vez mais complicado, caracterizado por diversos obstáculos que afetam a eficiência na coleta, conservação e avaliação de provas digitais.

A vasta quantidade e diversidade de informações geradas incessantemente por sensores, câmeras, assistentes virtuais e wearables transforma a identificação de dados relevantes em um procedimento extremamente complexo e técnico. Além disso, a variedade de sistemas e formatos, a volatilidade das informações e as restrições causadas por criptografia e acesso controlado dificultam as investigações periciais. A localização dispersa dos dados, frequentemente alojados em dispositivos locais, servidores em nuvem e data centers ao redor do mundo, aumenta ainda mais a complexidade da cadeia de custódia e requer cooperação entre diferentes jurisdições. Por outro lado, existe uma delicada relação entre a necessidade de conduzir investigações e a proteção da privacidade dos cidadãos, levando em conta a Lei Geral de Proteção de Dados (LGPD) e regulamentos internacionais.

Nesse cenário, emerge a principal questão desta pesquisa: entender como a variedade, instabilidade e complexidade dos dados em ambientes de IoT influenciam diretamente as metodologias forenses para a coleta, preservação e análise de evidências digitais.

O **grande volume de dados** gerado por dispositivos IoT representa um dos principais desafios para a perícia digital. Equipamentos como sensores, câmeras, relógios inteligentes e assistentes digitais produzem um fluxo constante de dados em diferentes formatos, que englobam registros, gravações de som, vídeos e informações biométricas. As tecnologias relacionadas à Internet das Coisas geram uma quantidade colossal de dados, frequentemente em tempo real, que podem ser trocados entre vários dispositivos, redes e plataformas de nuvem.

A imensidão dessa base de dados torna a seleção e a filtragem das informações relevantes um empreendimento bastante complicado, exigindo abordagens avançadas para a extração e a análise forense. O profissional deve identificar, dentre um milhão de registros, aqueles que possuem importância legal, garantindo a conservação da integridade e da autenticidade das evidências.

A **diversidade de dispositivos e formatos** influencia de maneira significativa a realização de investigações digitais. Cada usuário adota sistemas operacionais, protocolos de comunicação e estruturas de armazenamento particulares, muitas vezes desconsiderando os padrões forenses reconhecidos. Essa diversidade exige que os profissionais forenses tenham à disposição ferramentas e conhecimentos específicos para cada tipo de dispositivo, o que torna mais desafiadora a formulação de um método unificado para a análise forense em IoT.

Ademais, à medida que os dispositivos de IoT incorporam tecnologias modernas, como 5G e computação de borda, o panorama forense precisará se adaptar para considerar os

padrões de comportamento e os fluxos de dados únicos desses dispositivos em contextos mais sofisticados.

A **volatilidade das evidências digitais** representa um desafio, a natureza temporária de grande parte dos registros gerados por dispositivos conectados constitui um obstáculo, como muitos equipamentos operam com pouca memória, eles tendem a sobrescrever logs em curtos intervalos, o que torna indispensável a atuação rápida de quem precisa preservar informações potencialmente relevantes.

Os registros de eventos, como ilustração, podem ser apagados em questão de horas, comprometendo a obtenção de informações essenciais para investigações. Essa particularidade cria a necessidade de reações rápidas, protocolos para a preservação imediata e a implementação de tecnologias que minimizem a perda de dados efêmeros.

O **acesso restrito e a criptografia** representam um desafio contínuo entre segurança e pesquisa. Dispositivos conectados à Internet costumam utilizar métodos de proteção que envolvem técnicas sofisticadas de criptografia e sistemas de autenticação específicos, onde o acesso depende de chaves ou permissões fornecidas pelo fabricante. As medidas de segurança adotadas nesses dispositivos, como a aplicação de criptografia e a implementação de protocolos de autenticação, podem dificultar as investigações forenses. Embora sejam essenciais para garantir a integridade das informações e a privacidade dos usuários, essas abordagens criam obstáculos para os profissionais forenses que tentam acessar e analisar os dados.

Alcançar um ponto de equilíbrio entre a exigência de investigações forenses e a salvaguarda dos direitos de privacidade das pessoas continua sendo um desafio complexo, necessitando o desenvolvimento de estratégias que levem em conta tanto aspectos técnicos quanto éticos.

Outro desafio é a **distribuição geográfica dos dados**, característica intrínseca da arquitetura da IoT. As informações coletadas podem estar fragmentadas entre o dispositivo físico, servidores em nuvem do fabricante e centros de dados localizados em diferentes países.

A localização geográfica impõe desafios jurídicos e logísticos à coleta e conservação de evidências, especialmente quando há disparidades nas legislações de diferentes países e nas normas de proteção à privacidade. Portanto, a cooperação entre nações, juntamente com o estabelecimento de acordos para o intercâmbio de dados, torna-se fundamental para a efetividade da investigação digital.

A **cadeia de custódia** em ambientes de IoT configura-se como um procedimento complicado e de difícil supervisão. A diversidade de participantes, como produtores, provedores de nuvem, operadoras de rede e consumidores, torna a missão de monitorar as evidências mais propensa a falhas.

No aspecto técnico, é fundamental que qualquer prova digital, ou mesmo uma possível indicação digital, seja manipulada de acordo com práticas forenses reconhecidas. O National Institute of Standards and Technology (NIST), ao publicar a Special Publication 800-86, delineou quatro etapas que devem guiar esse processo: coleta, exame, análise e documentação final.

Além disso, o documento RFC 3227 (Request for Comments 3227: Diretrizes para a coleta e arquivamento de evidências) oferece recomendações importantes sobre como realizar a coleta e a preservação de evidências digitais. Ele recomenda que as instituições estabeleçam um procedimento de coleta sistemático, com o objetivo de tornar o processo o mais objetivo possível e evitar decisões precipitadas durante a sua execução.

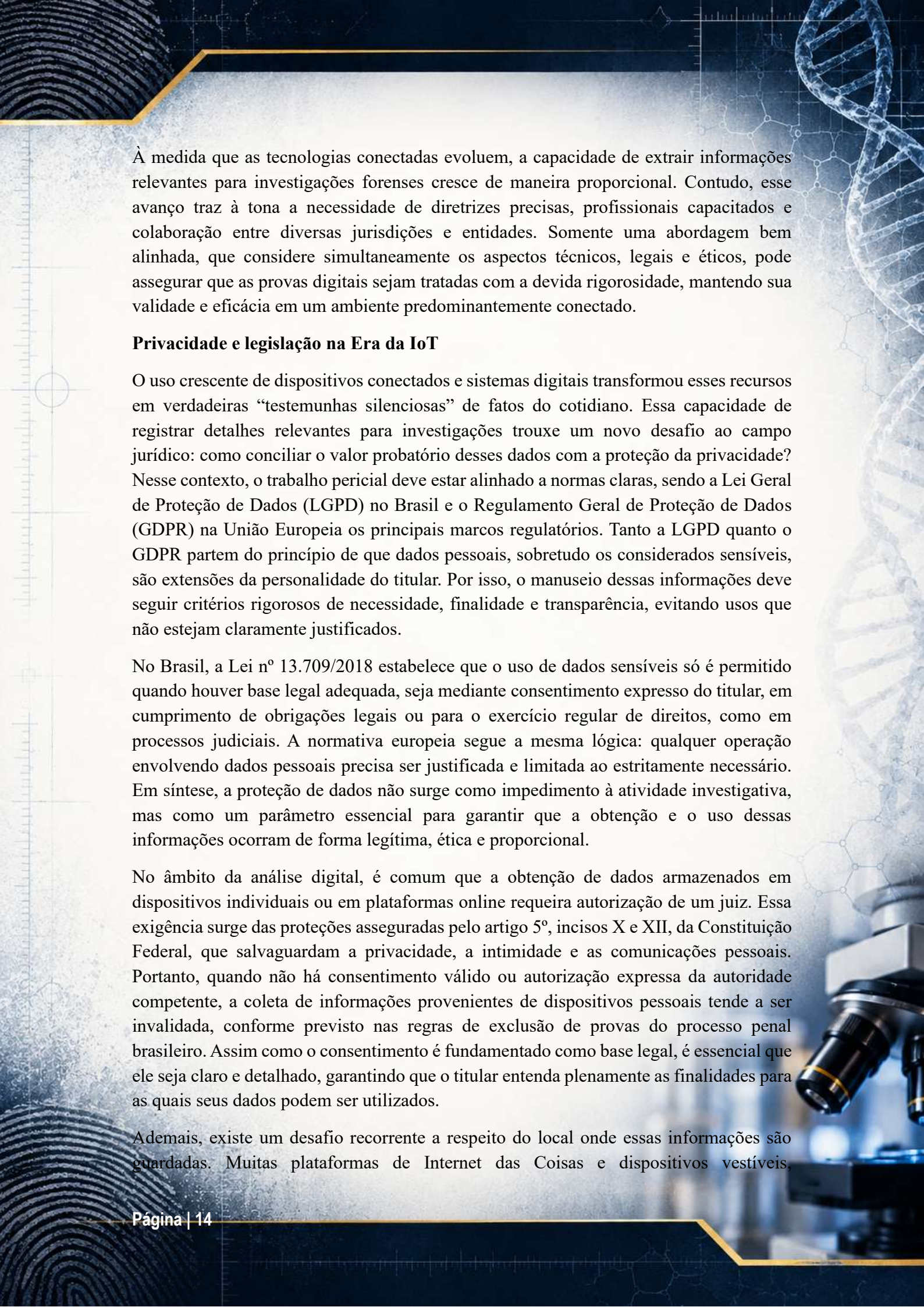
Para complementar essas recomendações, a norma ABNT NBR ISO/IEC 27037:2013 define os passos iniciais no manejo de evidências digitais, destacando quatro etapas principais: identificação, coleta, aquisição e preservação.

Em estudos conduzidos pelo NIST, foi sugerido um modelo conceitual que foca nas ferramentas de análise forense digital. O objetivo é estabelecer uma estrutura que possibilite a avaliação sistemática de possíveis falhas em cada fase do processamento, assegurando uma maior confiança na validação dessas ferramentas. Este modelo explora o processo interno das aplicações, oferecendo uma “ferramenta forense digital conceitual” que retoma a ideia de níveis de abstração. Assim, torna-se viável observar como as etapas se interligam, identificar onde podem ocorrer falhas e como elas podem se espalhar durante o processo. O estudo também apresenta um exemplo prático, com dados documentados conforme o padrão CASE (Cyber Investigation Analysis Standard Expression), demonstrando a aplicação prática dessa metodologia.

A cadeia de custódia em IoT requer uma abordagem de “triagem de emergência”. Para assegurar a integridade e autenticidade dos dados, é necessário um registro meticuloso de cada fase, desde a coleta até o armazenamento e análise. Nesse cenário, normas técnicas e legislações são fundamentais para uniformizar os procedimentos e garantir a validade das evidências digitais.

A **admissibilidade dessas provas** em juízo é o objetivo final que rege todo o processo pericial, exigindo uma demonstração inequívoca de autenticidade, integridade e legalidade.

Em ambientes de Internet das Coisas, os dados costumam estar espalhados entre múltiplos dispositivos, serviços em nuvem e sistemas de computação distribuída, em vez de estarem concentrados em um único local. Essa estrutura descentralizada cria desafios para aqueles que devem reconstruir eventos durante uma investigação, uma vez que as informações se tornam fragmentadas e distantes. Nesses cenários, garantir a integridade e a continuidade dos dados é crucial para que as evidências possam ser consideradas legítimas e admissíveis em processos jurídicos.



À medida que as tecnologias conectadas evoluem, a capacidade de extrair informações relevantes para investigações forenses cresce de maneira proporcional. Contudo, esse avanço traz à tona a necessidade de diretrizes precisas, profissionais capacitados e colaboração entre diversas jurisdições e entidades. Somente uma abordagem bem alinhada, que considere simultaneamente os aspectos técnicos, legais e éticos, pode assegurar que as provas digitais sejam tratadas com a devida rigorosidade, mantendo sua validade e eficácia em um ambiente predominantemente conectado.

### **Privacidade e legislação na Era da IoT**

O uso crescente de dispositivos conectados e sistemas digitais transformou esses recursos em verdadeiras “testemunhas silenciosas” de fatos do cotidiano. Essa capacidade de registrar detalhes relevantes para investigações trouxe um novo desafio ao campo jurídico: como conciliar o valor probatório desses dados com a proteção da privacidade? Nesse contexto, o trabalho pericial deve estar alinhado a normas claras, sendo a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia os principais marcos regulatórios. Tanto a LGPD quanto o GDPR partem do princípio de que dados pessoais, sobretudo os considerados sensíveis, são extensões da personalidade do titular. Por isso, o manuseio dessas informações deve seguir critérios rigorosos de necessidade, finalidade e transparência, evitando usos que não estejam claramente justificados.

No Brasil, a Lei nº 13.709/2018 estabelece que o uso de dados sensíveis só é permitido quando houver base legal adequada, seja mediante consentimento expresso do titular, em cumprimento de obrigações legais ou para o exercício regular de direitos, como em processos judiciais. A normativa europeia segue a mesma lógica: qualquer operação envolvendo dados pessoais precisa ser justificada e limitada ao estritamente necessário. Em síntese, a proteção de dados não surge como impedimento à atividade investigativa, mas como um parâmetro essencial para garantir que a obtenção e o uso dessas informações ocorram de forma legítima, ética e proporcional.

No âmbito da análise digital, é comum que a obtenção de dados armazenados em dispositivos individuais ou em plataformas online requeira autorização de um juiz. Essa exigência surge das proteções asseguradas pelo artigo 5º, incisos X e XII, da Constituição Federal, que salvaguardam a privacidade, a intimidade e as comunicações pessoais. Portanto, quando não há consentimento válido ou autorização expressa da autoridade competente, a coleta de informações provenientes de dispositivos pessoais tende a ser invalidada, conforme previsto nas regras de exclusão de provas do processo penal brasileiro. Assim como o consentimento é fundamentado como base legal, é essencial que ele seja claro e detalhado, garantindo que o titular entenda plenamente as finalidades para as quais seus dados podem ser utilizados.

Ademais, existe um desafio recorrente a respeito do local onde essas informações são guardadas. Muitas plataformas de Internet das Coisas e dispositivos vestíveis,

frequentemente, armazenam seus dados em servidores situados em outros países, os quais estão sujeitos a legislações e políticas de privacidade estrangeiras. Nesses casos, o acesso a essas informações é condicionado por mecanismos de cooperação internacional que assegurem a conformidade com as normas de proteção de dados e a soberania legal das nações envolvidas. A falta de cumprimento dessas etapas pode enfraquecer a validade da evidência e prejudicar a confiabilidade da avaliação pericial.

Para que as informações adquiridas por meio dessas tecnologias sejam empregadas de forma legítima em ações judiciais, o perito precisa garantir que os dados mantenham sua integridade, autenticidade e que sejam passíveis de rastreamento. É essencial documentar meticulosamente cada etapa do procedimento para manter a cadeia de custódia intacta e permitir a verificação do processo por terceiros. Assim, a função do perito digital se estende além de sua expertise técnica: ele serve como um elo entre a tecnologia e o sistema judiciário, convertendo registros complexos em dados claros e sólidos do ponto de vista legal, sempre levando em conta as consequências éticas relacionadas ao manuseio de informações profundamente conectadas à privacidade das pessoas.

Os princípios fundamentais da LGPD e do GDPR garantem que a análise digital se atenha aos critérios do processo legal apropriado: necessidade, finalidade e proporcionalidade. Transformar dados discretos e sutis em informações relevantes demanda cuidado: é crucial observar o que os sistemas expõem sem violar o que precisa permanecer confidencial. Nesse equilíbrio entre técnica e ética, a evidência digital torna-se válida e contribui para a formação de uma Justiça que se adapta às novas realidades da era interconectada.

### **O ecossistema de evidências das testemunhas invisíveis e sua relevância para perícia: os vestíveis e IoT não falam, mas registram, o papel do perito digital em transformar esses dados em evidências confiáveis**

A disseminação da Internet das Coisas (IoT) e a popularidade de dispositivos vestíveis, como smartwatches e sensores corporais, trouxeram uma nova relevância para itens do dia a dia, os quais agora têm a capacidade de coletar e transmitir informações de forma constante. Esses aparelhos, ao se comunicarem entre si e com plataformas de armazenamento em nuvem, atuam como testemunhas discretas, capturando hábitos, padrões de movimentação, interações e contextos de utilização quase em tempo real. O tipo de informação gerada por eles tem se revelado extremamente útil em investigações criminais, litígios civis, questões trabalhistas e também em diagnósticos médicos.

Por outro lado, a multiplicidade de marcas, formatos de arquivo e protocolos de comunicação gera um cenário bastante desafiador para quem precisa coletar, interpretar e validar essas informações. Nesse cenário, o perito digital exerce papel fundamental: transformar registros essencialmente técnicos em informações compreensíveis, confiáveis e juridicamente aceitáveis, preservando sempre a integridade, autenticidade e rastreabilidade das evidências.

Os dados coletados por dispositivos vestíveis e sistemas de Internet das Coisas constituem registros contínuos e automatizados que são, em grande parte, imunes a intervenções por parte dos usuários. Esses dados capturam com precisão a temporalidade de diversas métricas, incluindo informações fisiológicas, ambientais e comportamentais. Elementos como a frequência cardíaca, os padrões de movimento, a localização geográfica, as variáveis biométricas, os registros de interações com dispositivos e sensores contextuais podem ser utilizados para criar cronologias de eventos passados, validar álbis, identificar vítimas ou suspeitos, além de estabelecer correlações com outras fontes digitais. No âmbito da perícia, esses dados ganham importância legal quando passam por procedimentos rigorosos de coleta, manutenção da cadeia de custódia, análise técnica baseada em métodos científicos e interpretação contextual que respeita as diretrizes legais e os princípios da ciência forense.

Para que isso aconteça, a atuação pericial não deve restringir-se apenas ao conhecimento técnico. É fundamental compreender também as questões legais e metodológicas que guiam a utilização desses dados no sistema judicial, assegurando que cada fase atenda às exigências necessárias para que as informações sejam aceitas como evidência legítima.

**Tabela 1** – Dispositivos IoT e Vestíveis: tipos de dados e relevância forense

| Dispositivo                                                                         | Tipo de dado coletado                                                                           | Relevância Forense                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vestíveis de saúde e fitness (Smartwatches, pulseiras fitness, monitores cardíacos) | Frequência cardíaca, passos, localização GPS, padrões de sono, calorias, registro de movimento. | Pode sinalizar a localização ou falta dela em um determinado lugar, o momento de falecimento ou atividade física anterior a um acontecimento, além da condição física ou emocional da vítima ou do suspeito. |
| Smartphone                                                                          | Geolocalização, chamadas, mensagens, histórico de aplicativos, comandos de voz, fotos e vídeos. | Fundamental na pesquisa — mostra hábitos, conexões, movimentações, interações e pode relacionar acontecimentos com anotações de outras origens.                                                              |
| Assistentes domésticos inteligentes (Alexa, Google Home, Siri)                      | Comandos de voz, horários de interação, gravações de áudio, automações domésticas.              | Pode comprovar presença de pessoas, sequência de eventos ou emissão de comandos suspeitos (como acender lâmpadas, reproduzir música, abrir fechaduras).                                                      |
| Veículos conectados/smart cars                                                      | Rotas GPS, velocidade, travamento de portas, sensores de colisão, logs de ignição.              | Importantes para reconstituir rotas, investigar acidentes e confirmar movimentos vinculados a delitos.                                                                                                       |
| Câmeras e câmeras inteligentes                                                      | Vídeos, horários de detecção de movimento, reconhecimento facial.                               | Fornecem registro visual direto de ações e atividades e validação de comparecimento ou deslocamento em determinados lugares.                                                                                 |

|                                                                                                                              |                                                                                                             |                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Dispositivos médicos conectados                                                                                              | Dados vitais (pressão arterial, glicemia, oxigenação), alertas de emergência.                               | É possível apontar condições de saúde que ocorreram antes de situações críticas, como ataques cardíacos, envenenamentos ou consumo de substâncias. |
| Sensores domésticos (luzes, temperatura, portas, alarmes)                                                                    | Registros de ativação, temperatura, abertura/fechamento, consumo de energia.                                | Possibilitam a reconstrução da sequência de acontecimentos em uma casa (por exemplo: o momento em que uma porta foi aberta).                       |
| Roteadores e hubs IoT                                                                                                        | Logs de conexão de dispositivos, endereços IP, horários de acesso.                                          | Essenciais para definir a autoria digital, conexão de aparelhos e reconhecimento de invasões.                                                      |
| Brinquedos inteligentes e baby monitors (Babá eletrônica smart, brinquedos conectados)                                       | Áudio, vídeo, interação infantil                                                                            | Investigação de maus-tratos, invasões de privacidade, vigilância.                                                                                  |
| Dispositivos de localização e segurança pessoal (AirTag, Tile, rastreadores GPS, Botões de pânico, wearables anti-violência) | Posicionamento, histórico de rotas, proximidade com dispositivos. GPS, sinais de socorro, logs de ativação. | Rastreamento de vítimas ou suspeitos, detecção de perseguição ou sequestro, localização de objetos relevantes.                                     |

**Fonte:** Elaboração própria (2025)

O conjunto desses registros forma um ecossistema integrado de dados que, quando correlacionado, fortalece a narrativa probatória. Assim, a perícia digital em IoT e vestíveis não se limita à extração técnica, mas envolve análise contextual e correlação interdisciplinar, tornando o perito um intérprete da linguagem silenciosa das máquinas.

### Possíveis propostas e soluções tecnológicas

Em um cenário digital que se torna progressivamente mais intrincado, tecnologias emergentes estão se posicionando como parceiras na melhoria das práticas forenses e na construção da credibilidade em relação às evidências digitais. Entre as principais inovações estão a blockchain, a inteligência artificial e as iniciativas globais de padronização, que têm sido implementadas para aumentar a segurança, a verificabilidade e a consistência técnica dos processos.

O emprego de **blockchain** na custódia das provas garante que as evidências digitais permaneçam intactas e estáveis, registrando de maneira descentralizada cada fase do manuseio da evidência, desde a coleta até o arquivamento e a apresentação judicial. A utilização de mecanismos de registro distribuído, como blockchain, tem sido explorada como forma de registrar cada operação realizada sobre a evidência, criando um histórico

imutável e auditável. Isso reduz disputas sobre manipulação posterior e facilita a verificação independente dos metadados associados ao arquivo.

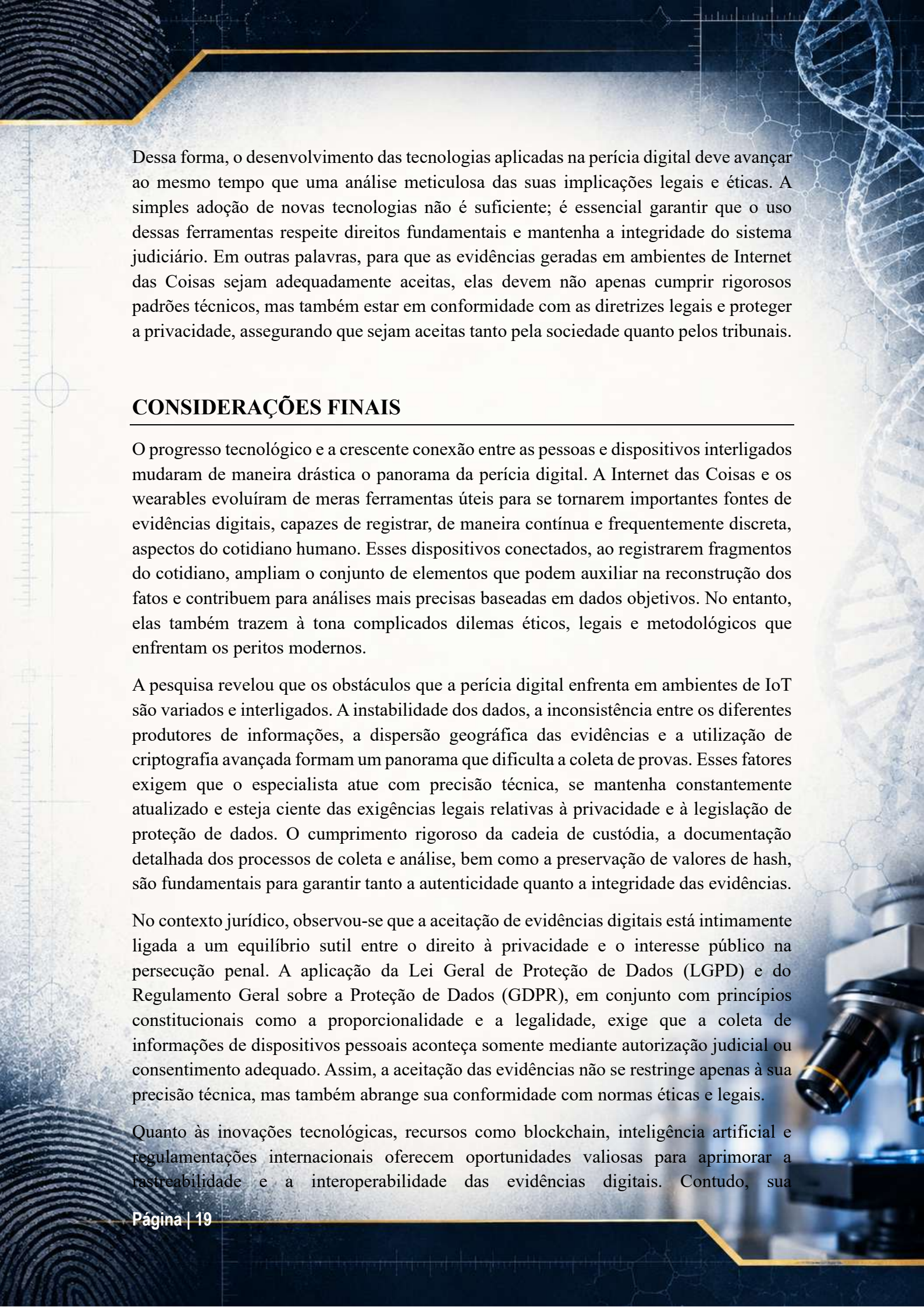
A implementação de tecnologias como **blockchain**, **inteligência artificial** e **a padronização global** trazem melhorias significativas para a perícia digital, porém essas inovações também levantam questões éticas e limitações práticas que precisam ser analisadas com atenção. No caso do blockchain, embora ele ofereça a permanência e a rastreabilidade das evidências, há preocupações relacionadas à privacidade dos dados que são armazenados, especialmente quando se lida com informações pessoais delicadas em sistemas descentralizados. Assim, é essencial encontrar um equilíbrio entre a transparência das evidências e a proteção dos dados pessoais, o que requer a criação de protocolos que garantam a anonimização e o controle de acesso, evitando a exposição indevida das informações dos usuários.

A aplicação de **inteligência artificial** na triagem de registros e na análise de padrões oferece uma solução eficiente para gerenciar o elevado volume e a complexidade dos dados provenientes de dispositivos IoT. Através de algoritmos de aprendizado de máquina, é possível detectar padrões suspeitos, identificar comportamentos anômalos e estabelecer conexões entre diferentes eventos. Esses algoritmos trabalham de maneira automatizada para processar informações repetitivas e para ressaltar registros que contêm evidências significativas, sem, contudo, dispensar a imprescindível supervisão humana.

Entretanto, a adoção de algoritmos de aprendizado de máquina para a filtragem de logs e a análise de padrões levanta preocupações relativas a possíveis preconceitos e erros de categorização. Modelos que não receberam um treinamento adequado ou que utilizam dados que não são completos podem levar a interpretações equivocadas, afetando a avaliação das evidências e a confiança nas análises periciais. Ademais, a automação não substitui a análise crítica de um especialista; ao contrário, ela exige que os profissionais estejam cientes das limitações e suposições inerentes a cada algoritmo, necessitando de uma supervisão humana meticulosa.

A **padronização internacional de procedimentos e formatos forenses** garante interoperabilidade entre sistemas, ferramentas e jurisdições. Normas como ISO/IEC 27037, 27041 e 27043 fornecem orientações detalhadas para a descoberta, coleta, retenção e aprovação de provas digitais. A uniformização desses critérios promove a colaboração internacional, melhora a consistência nas metodologias e reforça a aceitação legal das evidências.

A padronização a nível internacional é fundamental para a interoperabilidade e a aceitação legal das provas, mas enfrenta desafios devido à variação nas normas entre nações e à rápida mudança tecnológica. Vários dispositivos de IoT ainda funcionam sem seguir normas forenses bem estabelecidas, o que pode afetar a uniformidade nas investigações. A adoção global dessas normas requer um esforço conjunto entre agências reguladoras, fabricantes e as comunidades técnicas, o que exige tempo e negociação política.



Dessa forma, o desenvolvimento das tecnologias aplicadas na perícia digital deve avançar ao mesmo tempo que uma análise meticulosa das suas implicações legais e éticas. A simples adoção de novas tecnologias não é suficiente; é essencial garantir que o uso dessas ferramentas respeite direitos fundamentais e mantenha a integridade do sistema judiciário. Em outras palavras, para que as evidências geradas em ambientes de Internet das Coisas sejam adequadamente aceitas, elas devem não apenas cumprir rigorosos padrões técnicos, mas também estar em conformidade com as diretrizes legais e proteger a privacidade, assegurando que sejam aceitas tanto pela sociedade quanto pelos tribunais.

## CONSIDERAÇÕES FINAIS

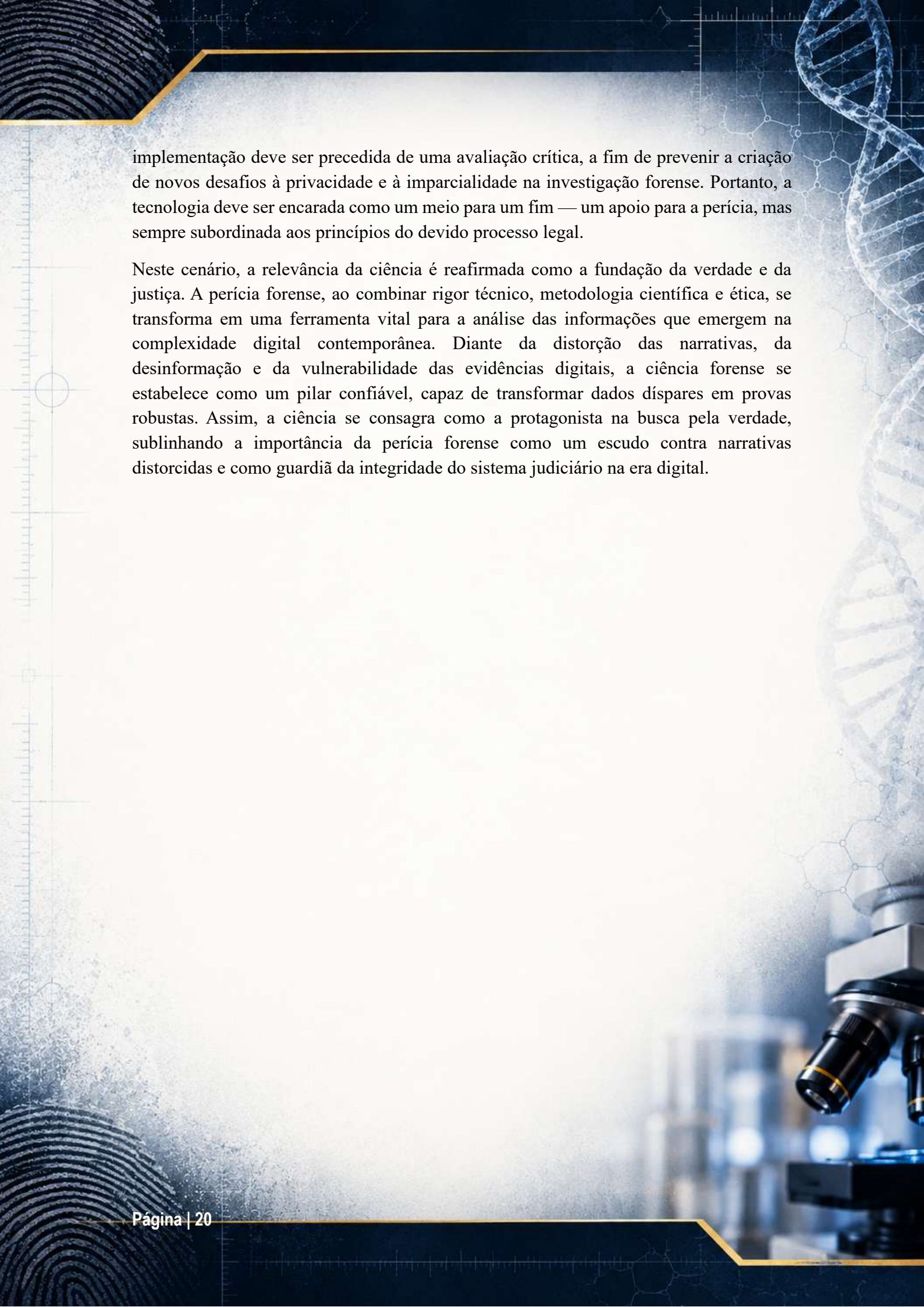
---

O progresso tecnológico e a crescente conexão entre as pessoas e dispositivos interligados mudaram de maneira drástica o panorama da perícia digital. A Internet das Coisas e os wearables evoluíram de meras ferramentas úteis para se tornarem importantes fontes de evidências digitais, capazes de registrar, de maneira contínua e frequentemente discreta, aspectos do cotidiano humano. Esses dispositivos conectados, ao registrarem fragmentos do cotidiano, ampliam o conjunto de elementos que podem auxiliar na reconstrução dos fatos e contribuem para análises mais precisas baseadas em dados objetivos. No entanto, elas também trazem à tona complicados dilemas éticos, legais e metodológicos que enfrentam os peritos modernos.

A pesquisa revelou que os obstáculos que a perícia digital enfrenta em ambientes de IoT são variados e interligados. A instabilidade dos dados, a inconsistência entre os diferentes produtores de informações, a dispersão geográfica das evidências e a utilização de criptografia avançada formam um panorama que dificulta a coleta de provas. Esses fatores exigem que o especialista atue com precisão técnica, se mantenha constantemente atualizado e esteja ciente das exigências legais relativas à privacidade e à legislação de proteção de dados. O cumprimento rigoroso da cadeia de custódia, a documentação detalhada dos processos de coleta e análise, bem como a preservação de valores de hash, são fundamentais para garantir tanto a autenticidade quanto a integridade das evidências.

No contexto jurídico, observou-se que a aceitação de evidências digitais está intimamente ligada a um equilíbrio sutil entre o direito à privacidade e o interesse público na persecução penal. A aplicação da Lei Geral de Proteção de Dados (LGPD) e do Regulamento Geral sobre a Proteção de Dados (GDPR), em conjunto com princípios constitucionais como a proporcionalidade e a legalidade, exige que a coleta de informações de dispositivos pessoais aconteça somente mediante autorização judicial ou consentimento adequado. Assim, a aceitação das evidências não se restringe apenas à sua precisão técnica, mas também abrange sua conformidade com normas éticas e legais.

Quanto às inovações tecnológicas, recursos como blockchain, inteligência artificial e regulamentações internacionais oferecem oportunidades valiosas para aprimorar a rastreabilidade e a interoperabilidade das evidências digitais. Contudo, sua

The background of the page is a composite image. On the left, there is a large, detailed fingerprint. On the right, a DNA double helix structure is visible, extending from the top to the bottom. In the bottom right corner, a portion of a microscope is shown, focusing on a sample. The overall color scheme is dark blue and black, with white and light blue highlights.

implementação deve ser precedida de uma avaliação crítica, a fim de prevenir a criação de novos desafios à privacidade e à imparcialidade na investigação forense. Portanto, a tecnologia deve ser encarada como um meio para um fim — um apoio para a perícia, mas sempre subordinada aos princípios do devido processo legal.

Neste cenário, a relevância da ciência é reafirmada como a fundação da verdade e da justiça. A perícia forense, ao combinar rigor técnico, metodologia científica e ética, se transforma em uma ferramenta vital para a análise das informações que emergem na complexidade digital contemporânea. Diante da distorção das narrativas, da desinformação e da vulnerabilidade das evidências digitais, a ciência forense se estabelece como um pilar confiável, capaz de transformar dados díspares em provas robustas. Assim, a ciência se consagra como a protagonista na busca pela verdade, sublinhando a importância da perícia forense como um escudo contra narrativas distorcidas e como guardião da integridade do sistema judiciário na era digital.

## REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS; ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. **NBR ISO/IEC 27037**: Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS; ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. **NBR ISO/IEC 27041**: Técnicas de segurança — Orientação para garantir a adequação e a suficiência do método investigativo de incidentes. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS; ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. **NBR ISO/IEC 27030**: Segurança em IoT - Fornece diretrizes para proteger dispositivos de Internet das Coisas (IoT), abordando riscos específicos. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS; ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. **NBR ISO/IEC 27042**: Avaliação de Evidências Digitais - Define métodos para avaliar a validade e confiabilidade de evidências digitais em investigações. 2016.

AHMED, Shams Forruque; SHAWON, Shanjana Shuravi; BHUYIAN, Afsana Bhuyian; GANDOMI, Amir H. **Forensics and security issues in the Internet of Things**. 2025. Disponível em: <https://doi.org/10.1007/s11276-025-03942-2>. Acesso em 14/10/2025.

AKINBI, Alex; MACDERMOTT, Áine; ISMAEL, Aras M. **A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models**. 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2666281722001512?via%3Dihub>. Acesso em: 29/10/2025.

ANDRADE, Ingrid Lima de. **Forense Digital aplicada ao combate de crimes cibernéticos: uma revisão**. 2024. Disponível em: 10.54751/revistafoco.v17n7-152. Acesso em: 16/10/2025.

BABUN, Leonardo; SIKDER, Amit Kumar; ACAR, Abbas; ULUAGAC, A. **Selcuk. IoT Dots: A Digital Forensics Framework for Smart Environments**. 2018. Disponível em: <https://arxiv.org/abs/1809.00745>. Acesso em: 14/10/2025.

FRANCISCO, José Carlos Ferreira. **Análise Forense Digital à Aplicação MIFIT**. 2022. Tese de mestrado (Mestrado em Cibersegurança e Informática Forense) — Escola Superior de Tecnologia e Gestão-Instituto Politécnico de Leiria, Portugal. Disponível em: <http://hdl.handle.net/10400.8/8122>. Acesso em: 14/10/2025.

INTERNET ENGINEERING TASK FORCE. **RFC 3227**: Guidelines for evidence collection and archiving. Fremont, 2002. Disponível em: <https://www.ietf.org/rfc/rfc3227.txt>. Acesso em: 14/10/2025.

ITU, International Telecommunication Union. Statistics: Individuals using the internet. Disponível em: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>. Acesso em 14/10/2025.

MARTIN, Erik David; SUTHERLAND, Iain; KARGAARD, Joakim. **IoT Security and Forensics: A Case Study**. Departamento de Tecnologia da Informação, Instituto de Tecnologia Ramrao Adik. Índia, 2023. Disponível em: <https://www.researchgate.net/publication/356750268>. Acesso em: 29/10/2025.

MBIMBI, B., MURRAY, D., WILSON, M.. **IoT Forensics-Based on the Integration of a Permissioned Blockchain Network**. 2024. Disponível em: <https://doi.org/10.3390/blockchains2040021>. Acesso em: 29/10/2025.

MEGAS, Katerina; FAGAN, Michael; CUTHILL, Bárbara; HOEHN, Brad; LEMIRE, David; HEROLD, Rebecca. **Workshop Summary Report for “Building on the NIST Foundations: Next Steps in IoT Cybersecurity”**. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency

or Internal Report (IR) NIST IR 8431. 2022. Disponível em: <https://doi.org/10.6028/NIST.IR.8431>. Acesso em: 09/10/2025.

MEGAS, Katerina; PICCARRETA, Ben; O'ROURKE, Danna Gabel. National Institute of Standards and Technology (NIST), **NISTIR 8201 Internet of Things (IoT) Cybersecurity Colloquium**. National Institute of Standards and Technology -NIST. 2017. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8201.pdf>. Acesso em: 25/10/2025.

National Institute of Standards and Technology. **An Abstract Model for Digital Forensic Analysis Tools A Foundation for Systematic Error Mitigation Analysis**. Gaithersburg: NIST, 2006. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-86/final>. Acesso em: 18/10/2025.

National Institute of Standards and Technology. **Guide to integrating forensic techniques into incident response**. NIST Special Publication 800-86. Gaithersburg: NIST, 2006. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-86/final>. Acesso em: 18/10/2025.

NERES, Winícius Ferraz. **A cadeia de custódia dos vestígios digitais sob a ótica da Lei n. 13.964/2019: aspectos teóricos e práticos**. 2021. Disponível em: <https://share.google/AcTkhXbFIGL4cOfHY>. Acesso em: 29/10/2025.

QUIST, Albert. **Digital Forensic Challenges in Internet of Things (IoT) Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics**. 2022. Disponível em: [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://fcc08321-8158-469b-b54df591e0bd3df4.filesusr.com/ugd/185b0a\\_f19bd1f0df32473ba002da998953db0b.pdf](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://fcc08321-8158-469b-b54df591e0bd3df4.filesusr.com/ugd/185b0a_f19bd1f0df32473ba002da998953db0b.pdf). Acesso em 16/10/2025.

RAMOS, José Ricardo Marcondes. **Ferramentas digitais forenses: Desenvolvimento e questões no contexto da aplicação da lei**. 2022. Disponível em: Boletim IBCCRIM - Ano 30 - N.º 361 - dezembro de 2022 - ISSN 1676-3661. Acesso em: 09/10/2025.

SCHNEIDER, Guilherme; ZORZO, Avelino Francisco; LUNARDI, Roben Castagna. **Modelo Integrado para Forense Computacional em cenários envolvendo aplicações IoT**. Rio Grande do Sul, 2023. Disponível em: <https://sol.sbc.org.br/index.php/sbseg/article/view/27195>. Acesso em: 16/10/2025.

SONI, Nishchal. **IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem**. *Computer and Telecommunication Engineering*. 2024; 2(4): 3070. Disponível em: <https://doi.org/10.54517/cte3070>. Acesso em: 16/10/2025.

ZANIOLO, Pedro Augusto. **Crimes Modernos, o impacto da tecnologia no Direito**. 5. ed. rev., ampl. e atual. – São Paulo: Editora Juspodivm, 2022.

CAPÍTULO

# 02

## DIVERSIFICAÇÃO NAS FORMAS DE APRESENTAÇÃO DE PRODUTOS CONTENDO THC: EXPERIÊNCIA DO LABORATÓRIO DE NARCÓTICOS DA POLÍCIA CIENTÍFICA DE GOIÁS

AUTORES

**Thaynara Lino Fernandes Alcântara**

**Jordana Costa Prata**

**André Cunha Amaral**

**Lara Cristina Teixeira**

Peritos Criminais, Laboratório de Narcóticos (LANARC),  
Instituto de Criminalística Leonardo Rodrigues,  
Polícia Científica do Estado de Goiás, Goiânia, GO

**Camila Bastos Ribeiro**

Perita Criminal, 10ª Coordenação Regional de Polícia Técnico-Científica  
de Anápolis, Polícia Científica do Estado de Goiás, Anápolis, GO



## DIVERSIFICAÇÃO NAS FORMAS DE APRESENTAÇÃO DE PRODUTOS CONTENDO THC: EXPERIÊNCIA DO LABORATÓRIO DE NARCÓTICOS DA POLÍCIA CIENTÍFICA DE GOIÁS

**Resumo:** A Cannabis sativa representa a substância ilícita de maior prevalência nas apreensões em Goiás. Este estudo caracteriza a diversidade morfológica e matricial de produtos contendo tetrahydrocannabinol (THC) analisados pelo Laboratório de Narcóticos da Polícia Científica de Goiás. Mediante análise retrospectiva de laudos periciais, identificaram-se cinco categorias principais: material vegetal, extratos oleosos, concentrados sólidos, produtos comestíveis e produtos industrializados. As análises laboratoriais empregaram cromatografia gasosa acoplada a espectrometria de massas e espectroscopia no infravermelho, confirmando presença inequívoca de THC em todas as categorias. A heterogeneidade observada relaciona-se a mudanças regulatórias internacionais, dinâmicas de mercado e difusão digital de conhecimento técnico. Esta diversificação impõe desafios analíticos significativos, demandando atualização metodológica, validação para matrizes complexas e capacitação técnica especializada dos peritos criminais.

**Palavras-chave:** Cannabis sativa; Tetrahydrocannabinol; Toxicologia forense

### INTRODUÇÃO

A Polícia Científica do Estado de Goiás possui em sua organização interna o Laboratório de Narcóticos (LANARC), sediado no Instituto de Criminalística Leonardo Rodrigues (ICLR) [1], responsável pelo recebimento, análise, armazenamento e destinação de drogas e substâncias correlatas provenientes dos 246 municípios do Estado de Goiás. São realizadas pelo LANARC exames preliminares de constatação de drogas e exames de identificação de drogas e substâncias correlatas, os quais demandam técnicas analíticas de alta complexidade. Com base nesses procedimentos, é possível a verificação da estrutura química e, posteriormente, a possibilidade do seu enquadramento como substância prosrita e ou controlada, conforme a Portaria nº. 344, de 12 de maio de 1998 do Ministério da Saúde.

A Cannabis sativa, popularmente conhecida como maconha, constitui a planta ilícita de maior cultivo, tráfico e consumo em escala global. No contexto brasileiro, e particularmente no Estado de Goiás, esta substância representa a droga de maior prevalência nas apreensões realizadas pelas forças de segurança pública. A planta Cannabis contém mais de 500 compostos químicos identificados, dos quais aproximadamente 60 pertencem à classe dos canabinoides terpenofenólicos. O Tetrahydrocannabinol é o principal responsável pelos efeitos psicoativos característicos da

substância, atuando como agonista parcial dos receptores canabinoides do sistema endocanabinoide humano.

Historicamente, o consumo tradicional de Cannabis limitava-se ao material vegetal prensado, plantas in natura e cigarros de fabricação artesanal. Contudo, os peritos criminais do LANARC têm observado uma tendência emergente nas formas de apresentação da maconha e documentado a diversificação expressiva nas características morfológicas e matriciais dos produtos contendo THC submetidos à perícia. Esta tendência emergente apresenta implicações diretas para a prática forense, demandando atualização metodológica, validação de técnicas analíticas para matrizes não convencionais e capacitação continuada dos profissionais.

## OBJETIVO

---

Compilar e apresentar as diferentes formas de apresentação da maconha que foram analisadas em 2025 pelo LANARC, de forma a dar ênfase na crescente variedade apreendida e orientar as demais forças de segurança pública sobre essa tendência.

## METODOLOGIA

---

Trata-se de estudo descritivo, documental e retrospectivo, com abordagem qualitativa, baseado em análise de laudos periciais. Foram revisados laudos periciais de exames de identificação de substância emitidos pelos peritos criminais do LANARC, referentes a apreensões de drogas e substâncias correlatas realizadas no território do Estado de Goiás. O período de análise compreendeu de janeiro a novembro de 2025, conforme disponibilidade no Sistema de Criminalística ODIN.

As análises periciais documentadas nos laudos revisados basearam-se em técnicas instrumentais consolidadas para identificação de canabinoides. A cromatografia gasosa acoplada à espectrometria de massas (CG/EM) foi utilizada como técnica de referência para identificação de substâncias controladas, permitindo separação cromatográfica dos compostos e identificação por padrão de fragmentação molecular característico. A espectroscopia no infravermelho foi empregada como técnica complementar baseada na absorção de radiação infravermelha por grupos funcionais específicos, gerando espectros vibracionais característicos para cada substância. A confirmação da presença de THC foi estabelecida mediante comparação dos perfis cromatográficos e espectrais obtidos com bibliotecas espectrais de referência e padrões certificados.

Os dados foram organizados por categorias de apresentação física, possibilitando caracterização descritiva da diversidade observada.

## RESULTADOS E DISCUSSÃO

A análise dos laudos periciais revelou diversidade substancial nas formas de apresentação de produtos contendo THC apreendidos no Estado de Goiás. As amostras puderam ser agrupadas em cinco categorias principais demonstradas a seguir:

A primeira categoria engloba os materiais vegetais tradicionais, incluindo material vegetal *in natura*, material vegetal prensado em blocos compactados, preservando estrutura morfológica original das inflorescências. Esta categoria permanece predominante numericamente nas apreensões, representando a forma tradicional de apresentação da substância.



**Ilustração 1.** Material vegetal *in natura* e prensado analisados pelo LANARC.

A segunda categoria compreende materiais semissólidos, de cor amarelada e de consistência pastosa.



**Ilustração 2.** Materiais pastosos e olecosos analisados pelo LANARC.

A terceira categoria corresponde a concentrados sólidos manifestando-se como material finamente pulverizado de cor branca e particulado de aspecto cristalino.



**Ilustração 3.** Material pulverizado e cristalizado analisados pelo LANARC.

A quarta categoria engloba produtos comestíveis, incluindo confeitos gelatinosos frequentemente apresentados em embalagens coloridas com dosagens indicadas, produtos alimentícios compactados incorporando extratos de Cannabis e outras preparações culinárias diversas.



**Ilustração 4.** Materiais comestíveis analisados pelo LANARC.

A quinta categoria corresponde a produtos industrializados com aspecto de legitimidade comercial, como unidades para consumo inalatório com aparência de produtos comerciais legítimos e preparações líquidas destinadas a dispositivos eletrônicos de vaporização com diversos aromas



**Ilustração 5.** Materiais industrializados analisados pelo LANARC.

As técnicas instrumentais empregadas permitiram identificação inequívoca de THC em amostras representativas de todas as categorias descritas, com perfis cromatográficos e espectrais apresentando concordância com padrões de referência certificados.

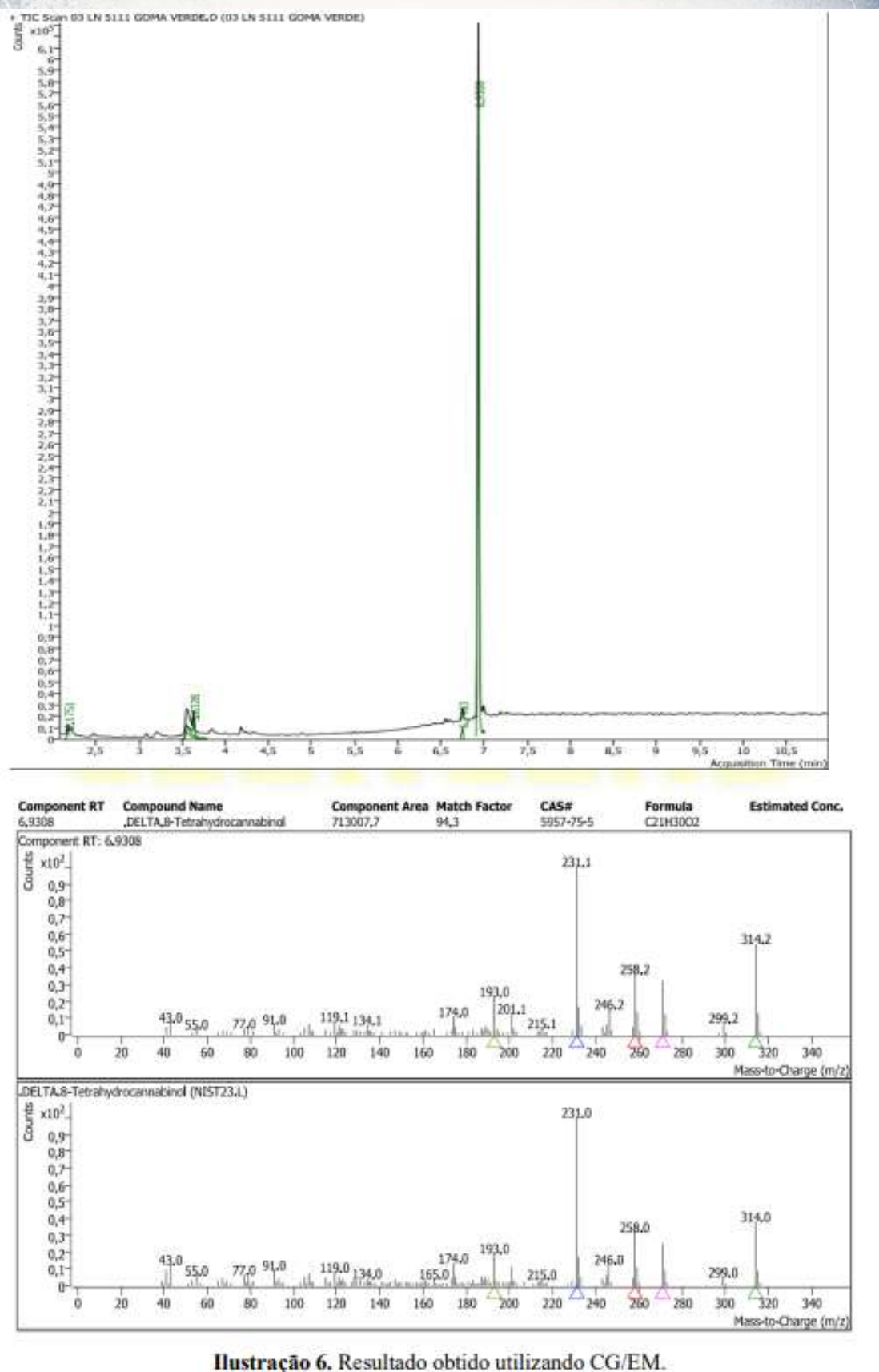
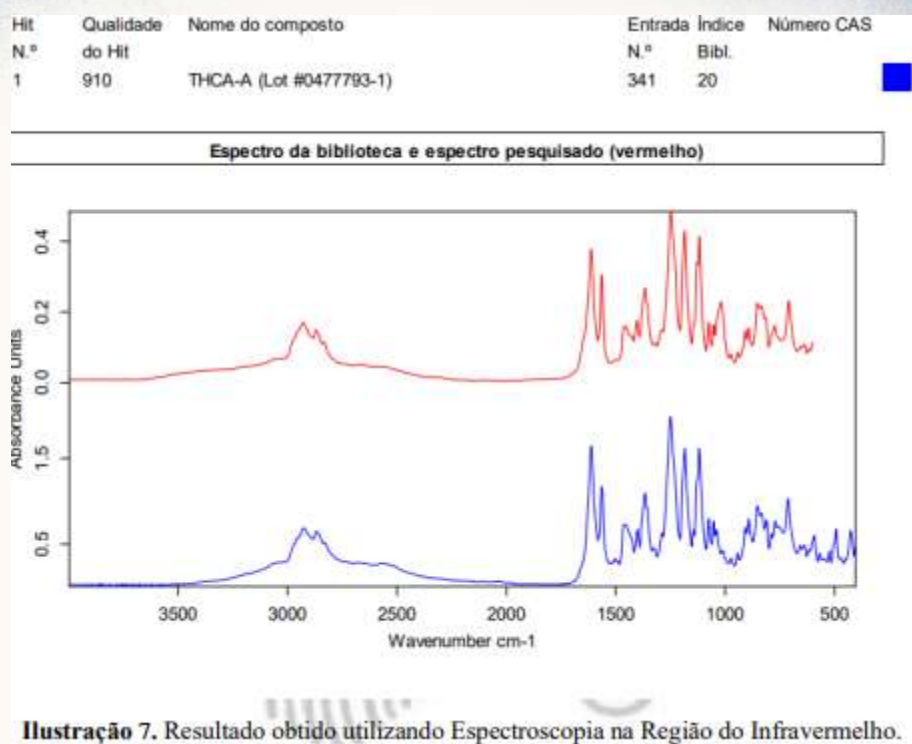


Ilustração 6. Resultado obtido utilizando CG/EM.



A heterogeneidade observada pode ser atribuída à convergência de múltiplos fatores estruturais. Nos últimos anos, diversos países implementaram políticas de legalização ou descriminalização da Cannabis, estimulando desenvolvimento de indústria legal sofisticada com investimentos em pesquisa, tecnologias de extração e formulações inovadoras. O mercado ilícito, embora operando à margem da legalidade, responde a lógicas econômicas tradicionais, adaptando ofertas para atender demandas heterogêneas de consumidores e maximizar margens de lucro através de produtos de maior valor agregado. Ainda, plataformas digitais desempenham papel catalisador na difusão de técnicas de extração caseira, informações sobre novas formas de consumo e marketing informal de produtos.

Esta diversificação impõe desafios significativos à perícia criminal, uma vez que a variabilidade matricial requer protocolos de preparação amostral específicos, componentes das matrizes podem atuar como interferentes na análise e produtos altamente concentrados demandam diluições adequadas para quantificação precisa. Torna-se imperativa a validação de métodos para matrizes não convencionais, o desenvolvimento de procedimentos de extração específicos para diferentes categorias de produtos e o estabelecimento de controles de qualidade adequados. A capacitação profissional representa pilar fundamental, demandando treinamento continuado em técnicas instrumentais avançadas, atualização sobre tendências globais no mercado de Cannabis e desenvolvimento de competências em interpretação toxicológica contextualizada dos resultados.

## CONSIDERAÇÕES FINAIS

O presente estudo documenta tendência clara de diversificação nas formas de apresentação de produtos contendo THC apreendidos no Estado de Goiás, evidenciando transição de um mercado historicamente centrado em material vegetal tradicional para cenário heterogêneo englobando materiais petrificados, cristalizados, produtos comestíveis e formulações industrializadas. Esta transformação, impulsionada por mudanças regulatórias globais, dinâmicas de mercado e difusão digital de conhecimento técnico, impõe desafios substanciais à perícia criminal.

Dessa forma, este estudo alcançou os objetivos definidos e as informações apresentadas representam uma ferramenta importante para a elaboração de estratégias para uma melhor gestão no combate às drogas de abuso no Estado de Goiás, visando orientar às demais forças de segurança pública a identificar novos padrões de apreensões de drogas. É imperioso que a Polícia Científica do Estado de Goiás se mantenha atenta e com sua capacidade técnica robusta e atualizada, essencial para resposta efetiva às transformações contínuas no fenômeno das drogas ilícitas e para produção de provas periciais de elevada qualidade técnico-científica.

## REFERÊNCIAS

- BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Portaria n. 344, de 12 de maio de 1998. Aprova o Regulamento Técnico sobre substâncias e medicamentos sujeitos a controle especial. Brasília, Diário Oficial da União (1998).
- BORDIN, D D, MESSIAS M, LANARO R, CAZENAVE S O S. Análise forense: pesquisa de drogas vegetais interferentes de testes colorimétricos para identificação dos canabinoides da maconha (*Cannabis sativa* L.). Química Nova. 2012;35(10).
- CERDÁ M, KILMER B. Uruguay's middle-ground approach to cannabis legalization. Int J Drug Policy. 2017;42:118-120
- ELSOHL MA, MEHMEDIC Z, FOSTER S, GON C, CHANDRA S. Changes in Cannabis Potency over the Last Two Decades (1995-2014). Biol Psychiatry. 2016;79(7):613-619.
- GOIÁS. Superintendência de Polícia Técnico Científica de Goiás. Portaria nº 181, de 15 de agosto de 2025. Estabelece a estrutura organizacional da Polícia Científica da Secretaria de Estado da Segurança Pública do Estado de Goiás – SSP e dá outras providências (2025).
- GOIÁS. Superintendência de Polícia Técnico Científica de Goiás. Manual de Requisição de Perícias. Goiânia, GO: Secretaria de Segurança Pública (2024).
- GOIÁS. Secretaria de Estado da Segurança Pública. Sistema de Criminalística ODIN (2025). Retirado em 18/11/2025, de <https://odin.ssp.go.gov.br/sistemas/odin/relatorios/periciaPeriodo.php>
- HU C, YIN M, LIU B, LI X, Detection of Illicit Drug Trafficking Events on Instagram: A Deep Multimodal Multilabel Learning Approach. ArXiv 2021, 2108.08920v2

MAURER, H H; PFLEGER, K; WEBER, A.A. Mass Spectral and GC Data of Drugs, Poisons, Pesticides, Polluants and Their Metabolites ®(4th). Weinheim, WILEY – VCH: Verlag GmbH e KGaA, v. 1, p. 4, 2011.

SUAREZ-JACOBO A, PACHECO A D, ALATORRE E B, CASTILLO-HERRERA G A, Cannabis Extraction Technologies: Impact of Research and Value Addition in Latin America. Molecules 2023, 28(7), 2895;

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Grupo De Pesquisa Em Polímeros E Manufatura Aditiva. Espectroscopia de Infravermelho. Disponível em: <https://policom.ufsc.br/espectroscopia-deinfravermelho/#:~:text=Espectroscopia%20no%20infravermelho%20por%20transformada,a%20investigar%20sua%20composi%C3%A7%C3%A3o%20qu%C3%ADmica>. Acesso: 18/11/2025.

UNODC (United Nations Office on Drugs and Crime). Laboratory and scientific section. Recommended Methods for the Identification and Analysis of Cannabis and Cannabis Products. Vienna: 2024.