Universidade do Contestado | www.unc.br/periodicos ISSNe: 2237-9010
ÁGORA REVISTA DE DIVULGAÇÃO CIENTÍFICA

INTEGRAÇÃO ENTRE ARQUIVÍSTICA E PERÍCIA DIGITAL: DESAFIOS, LEGISLAÇÃO E POLÍTICAS PÚBLICAS PARA EVIDÊNCIAS DIGITAIS

INTEGRATION BETWEEN ARCHIVAL SCIENCE AND DIGITAL FORENSICS: CHALLENGES, LEGISLATION, AND PUBLIC POLICIES FOR DIGITAL EVIDENCE

Gisele Maria Arcanjo[1]

RESUMO

O presente artigo analisa a integração entre perícia digital, teoria arquivística e tecnologia, com foco na gestão, preservação e autenticidade de documentos digitais. Parte-se do conceito de informação-como-coisa, de Buckland e Rondinelli, para discutir como dados, textos, documentos, objetos e eventos podem ser tratados como evidências digitais, considerando aspectos de autenticidade, fidedignidade e confiabilidade. São discutidos desafios práticos da perícia digital, como a rápida evolução tecnológica, diversidade de formatos, vulnerabilidades digitais (*ransomware, deepfakes*, uso de Inteligência Artificial na manipulação e detecção de conteúdos digitais) e a complexidade da coleta e preservação de provas em diferentes dispositivos e plataformas de armazenamento, incluindo a nuvem. O estudo destaca modelos como Digital Records Forensics (DRF) e a Cadeia de Preservação (CoP), que combinam arquivologia, direito e perícia digital para garantir integridade e validade jurídica dos registros digitais. A legislação brasileira sobre crimes digitais, incluindo o Marco Civil da Internet, LGPD, Lei Carolina Dieckmann e normas sobre estelionato eletrônico, criptoativos e proteção de crianças e adolescentes, é apresentada, evidenciando sua relevância para a prática pericial. Iniciativas institucionais, como o Projeto Chegando Junto e a atuação do Ministério Público de Minas Gerais (MPMG), demonstram a importância de políticas públicas e ações educativas para prevenir golpes digitais, em parceria com organizações internacionais, como a Global Anti-Scam Alliance (GASA). Por tratar-se de estudo conceitual e exploratório, suas conclusões não possuem generalização empírica, indicando a necessidade de pesquisas futuras sobre aplicação prática do modelo DRF/CoP. Conclui-se que a integração entre arquivística, perícia digital e tecnologia, aliada à atualização profissional e à atuação institucional, é essencial para assegurar a confiabilidade das evidências digitais, fortalecer o papel social das instituições e proteger a sociedade frente às ameaças cibernéticas.

Palavras-chave: perícia digital; arquivística; cibersegurança; políticas públicas; evidências digitais.

[1]Mestre em Ciência da Informação. Ministério Público do Estado de Minas Gerais. Contagem. Minas Gerais. Brasil. E-mail: arcanjo.gisele@gmail.com. ORCID: https://orcid.org/0000-0002-3229-7529.

ABSTRACT

This article examines the integration of digital forensics, archival theory, and technology, focusing on the management, preservation, and authenticity of digital documents. It draws on Buckland and Rondinelli's concept of information-as-thing to discuss how data, texts, documents, objects, and events can be treated as digital evidence, considering aspects of authenticity, reliability, and trustworthiness. The study addresses practical challenges in digital forensics, such as rapid technological evolution, format diversity, digital vulnerabilities (ransomware, deepfakes, and the use of Artificial Intelligence in content manipulation and detection), and the complexity of collecting and preserving evidence across devices and cloud-based platforms. It highlights models such as Digital Records Forensics (DRF) and the Preservation Chain (CoP), which combine archival science, law, and digital forensics to ensure the integrity and legal validity of digital records. Brazilian legislation on cybercrimes—including the Civil Rights Framework for the Internet, the General Data Protection Law (LGPD), the Carolina Dieckmann Law, and regulations related to electronic fraud, crypto-assets, and the protection of children and adolescents—is presented, emphasizing its relevance to forensic practice. Institutional initiatives, such as the Chegando Junto Project and the work of the Public Prosecutor's Office of Minas Gerais (MPMG), illustrate the importance of public policies and educational actions to prevent digital fraud, in partnership with international organizations such as the Global Anti-Scam Alliance (GASA). As this is a conceptual and exploratory study, its conclusions lack empirical generalizability, indicating the need for future research on the practical application of the DRF/CoP model. The article concludes that integrating archival science, digital forensics, and technology—combined with continuous professional development and institutional action—is essential to ensure the trustworthiness of digital evidence, strengthen the social role of institutions, and protect society against emerging cyber threats.

Key words: digital forensics; archival science; cybersecurity; public policies; digital evidence.

Artigo recebido em: 04/11/2025
Artigo aprovado em: 06/03/2026
Artigo publicado em: 09/03/2026
Doi: https://doi.org/10.24302/agora.v31.6136

1 INTRODUÇÃO

No cenário atual, a confiabilidade das evidências digitais tem sido cada vez mais questionada. Um exemplo emblemático ocorreu no Brasil, quando o advogado Michel França demonstrou, durante um julgamento, como é possível editar conversas do WhatsApp em tempo real usando ferramentas de desenvolvedor do próprio navegador. A apresentação viralizou nas redes sociais e expôs um problema

recorrente: a facilidade com que *prints* de tela podem ser manipulados, sem qualquer garantia sobre sua origem ou integridade (DireitoNews, 2023). Essa fragilidade evidencia a necessidade de métodos de coleta digital que sigam padrões periciais e assegurem a cadeia de custódia, garantindo a autenticidade dos registros desde sua origem até o momento em que são usados como prova.

Esse caso ilustra a importância da perícia digital, peça-chave para análise e validação de provas eletrônicas, especialmente em situações com alta complexidade técnica. Ela está diretamente ligada à arquivologia, que atua na gestão, preservação e garantia da autenticidade dos documentos digitais. A arquivologia contribui para assegurar integridade, cadeia de custódia e interpretação adequada do contexto dos documentos, estabelecendo critérios essenciais para avaliar a confiabilidade e proveniência das provas.

Segundo Rubin (2013):

> Fontes e Meios de prova: aqui estamos diante de outra diferenciação clássica na teoria geral da prova, em que os primeiros são os elementos (mecanismos) externos do processo aptos a provar; e os últimos são os elementos (mecanismos) internos do processo aptos a provar, ou seja, as formas pelas quais se podem produzir provas em juízo de acordo com a legislação processual do país (confissão, depoimento pessoal, interrogatório, testemunhas**, documentos**, perícia e inspeção judicial) (Rubin, 2013, online, grifo nosso)

Diante desses desafios, este estudo adota uma abordagem conceitual baseada na integração entre arquivologia e perícia digital, fundamentada em literatura especializada, projetos internacionais e legislação pertinente. Para orientar essa análise, o artigo adota a seguinte questão de pesquisa: de que maneira a integração entre teoria arquivística, práticas de perícia digital e instrumentos tecnológicos pode aprimorar a confiabilidade das evidências digitais no contexto brasileiro?

O objetivo é analisar como princípios como autenticidade, fidedignidade e confiabilidade podem ser assegurados na gestão e preservação de documentos digitais, considerando tanto aspectos teóricos quanto diretrizes práticas sugeridas por especialistas e iniciativas internacionais. “O arquivista, assim como o cientista pericial, faz perguntas sobre as características dos documentos e sobre seu uso — questões cada vez mais relevantes no ambiente digital” (Duranti, 1995, p. 6, tradução nossa).

Iniciativas como o projeto InterPARES Trust (ITrust), desenvolvido entre 2012 e 2019, reforçam essa perspectiva. O Projeto investigou como garantir confiança e

confiabilidade em documentos digitais. Com mais de cinquenta universidades e organizações de várias partes do mundo, incluindo América Latina, reúne especialistas de arquivologia, direito, tecnologia da informação, perícia digital e segurança cibernética. Suas contribuições criaram bases teóricas e metodológicas que sustentam políticas, normas e legislações voltadas à governança digital e à preservação da memória em ambientes computacionais complexos (Interpares Trust, 2019).

Este artigo é exploratório e qualitativo, o objetivo é promover o diálogo entre perícia digital, arquivologia e áreas correlatas, como direito e tecnologia da informação, para compreender desafios e práticas relacionados à gestão, preservação e autenticidade dos documentos digitais. Do ponto de vista metodológico, o estudo se caracteriza como análise conceitual, estruturada por revisão de literatura, exame de modelos teóricos consolidados — como *Digital Records Forensics* (DRF) e Cadeia de Preservação (CoP) — e contextualização normativa.

Além disso, o avanço recente da Inteligência Artificial amplia a complexidade do problema, sobretudo com a disseminação de *deepfakes*, sínteses automatizadas de voz e imagem e ferramentas capazes de alterar conteúdos digitais sem deixar rastros perceptíveis. Ao mesmo tempo, técnicas de IA também têm sido empregadas para apoiar a detecção de manipulações, reforçando a necessidade de integração entre tecnologia, perícia digital e teoria arquivística na validação das evidências.

Frente a esse cenário, torna-se fundamental compreender os fundamentos que sustentam a validade das evidências digitais, especialmente quando elas passam a ser tratadas como documentos arquivísticos. Assim, a integração entre perícia digital e arquivologia torna-se essencial para superar os desafios atuais e assegurar que as evidências digitais sejam aceitas e reconhecidas com segurança pelos sistemas judiciais.

Como principais achados, o estudo demonstra que a confiabilidade probatória depende de práticas articuladas entre Arquivística, Perícia Digital e Tecnologia, bem como da adoção de modelos formais de preservação capazes de complementar a cadeia de custódia tradicional.

Para orientar a leitura, o artigo organiza-se da seguinte forma: (a) apresenta os principais conceitos relacionados à confiabilidade, autenticidade, fidedignidade e cadeia de custódia; (b) discute o referencial teórico interdisciplinar; (c) analisa os

modelos DRF e CoP; (d) examina o cenário tecnológico e jurídico brasileiro; e (e) finaliza com as contribuições, limitações e recomendações para pesquisas futuras.

A seguir, são apresentados os principais conceitos envolvidos nesse debate, com foco nas relações entre confiabilidade, autenticidade, fidedignidade e cadeia de custódia.

2 CONCEITOS E DESAFIOS DA PERÍCIA DIGITAL NO CONTEXTO ARQUIVÍSTICO

A Lei Federal nº 8.159/1991, que institui a Política Nacional de Arquivos, determina em seu art. 1º que o Poder Público deve gerir e proteger os documentos de arquivo, reconhecendo-os como instrumentos essenciais de prova e informação para a administração pública.

Casey (2011, p. 7, tradução nossa) define que “A perícia digital é a aplicação de técnicas investigativas e análise computacional para coletar e preservar evidências digitais de modo adequado para apresentação em tribunal”. A autora também define que a “Evidência digital é qualquer dado armazenado ou transmitido por computador que apoie ou refute uma teoria sobre o delito, envolvendo elementos críticos como intenção ou álibi” (Casey, 2011, p.12, tradução nossa).

No entanto, a perícia digital enfrenta uma série de desafios práticos e conceituais que impactam sua aplicação no campo arquivístico. Entre os principais entraves estão a rápida evolução tecnológica, a diversidade e complexidade dos dispositivos e formatos digitais, além das limitações dos procedimentos periciais tradicionais frente às particularidades dos registros digitais. Segundo Rogers (2021):

> perícia digital se preocupa principalmente em identificar os objetos digitais e os traços ou rastros digitais desses objetos que podem servir como evidência de atividade criminosa e analisar esses objetos e aqueles vestígios de sua capacidade probatória. Então, eles estão procurando por atribuição a proveniência dos traços ou sua identidade e, então, é claro, mantendo sua integridade e verificabilidade ao longo do tempo para que possam servir como prova (Rogers, 2021, p. 2, tradução nossa).

No contexto arquivístico, um desafio crucial é a definição precisa do que constitui um documento digital autêntico e confiável, considerando as múltiplas camadas de metadados, registros de sistema e logs que podem acompanhar um

arquivo. A confiabilidade e autenticidade dos registros digitais devem ser avaliadas em conjunto, pois envolvem aspectos internos, externos e procedimentais. Contudo, esses elementos não garantem validade futura por si só. Ao longo da história, diferentes culturas buscaram formas de conferir confiabilidade a documentos, como testemunhas, objetos simbólicos ou chancela de autoridades. Tais práticas asseguram autenticidade, mas não necessariamente fidedignidade. Esta última está ligada à autoridade e credibilidade do produtor para relatar os fatos com precisão — um documento pode ser autêntico, mas não representar fielmente o que ocorreu (Duranti, 1995). O que nos leva a questão de um documento ser ou não imparcial.

Como observa Eastwood, ao retomar Jenkinson, os documentos de arquivo, por resultarem diretamente das ações que registram, são considerados imparciais, já que não foram criados para agradar ou informar a posteridade. Essa condição lhes confere autenticidade (confiabilidade como registro dos fatos), desde que não sofram alterações posteriores. Justamente por poderem revelar aspectos indesejados, devem ser protegidos contra corrupções e assegurar a preservação de sua imparcialidade. (2013, p. 21-22). Assim, um documento pode ser autêntico e imparcial, mesmo que contenha informações não confiáveis, mas não será considerado fidedigno.

Autenticidade assegura que o registro digital é genuíno, criado pela fonte legítima e sem alterações que comprometam sua integridade original, e a confiabilidade refere-se à estabilidade e consistência do registro ao longo do tempo, garantindo resistência a modificações não autorizadas (Duranti, 1998; Kruse; Heiser, 2002). Ainda de acordo com Eastwood (2013, p. 22), a autenticidade dos documentos de arquivo não se encontra neles próprios, mas nos procedimentos metodológicos que regem sua produção, manutenção e custódia. Nesse sentido, a teoria arquivística ultrapassa a análise do documento em si e considera também o contexto processual que assegura sua criação, preservação e transmissão ao longo do tempo por meio da cadeia de custódia.

A cadeia de custódia é o processo que documenta a manutenção e o histórico da evidência, fundamental para demonstrar que esta não foi alterada (Carrier, 2005, p. 14). A cadeia de custódia assegura que documentos sejam identificados corretamente, protegidos contra corrupção e mantidos com integridade pelos custodiadores e seus sucessores. Nos documentos digitais, embora cumpra requisitos legais e suporte a presunção de autenticidade, ela é insuficiente, pois depende de

dados circunstanciais e não das propriedades intrínsecas dos documentos, que mudam a cada processamento e podem ser alteradas por software ou hardware. Além disso, meios digitais estão sujeitos à degradação, exigindo avaliação contínua da durabilidade. Por isso, o projeto InterPARES propôs complementar a cadeia de custódia com uma cadeia de preservação, registrando dados essenciais que comprovem a identidade e integridade dos documentos digitais ao longo do tempo.

De acordo com Luz e Flores (2013) e Duranti e Preston (2008), a Cadeia de Preservação (CoP), desenvolvida pelo projeto InterPARES, complementa a cadeia de custódia, registrando informações sobre práticas de criação, manutenção e arquivamento de documentos digitais para sustentar sua autenticidade. Esse modelo abrange todas as etapas do ciclo de vida do documento — produção, manutenção, avaliação e preservação digital — enquanto a cadeia de custódia mantém o foco na guarda, proteção e manutenção, mesmo em sistemas informatizados de gestão ou preservação. (Quadro 1)

Quadro 1 – Atividades da Cadeia de Preservação (CoP)

Atividade da CoP (Duranti; Preston, 2008)	**Texto Função / Descrição Texto**
Gerenciar a estrutura da cadeia de preservação	Planejar e organizar a cadeia de preservação para manter a autenticidade e integridade dos documentos
Gerenciar o processo de criação dos documentos	Registrar as práticas dos criadores para sustentar a presunção de autenticidade
Gerenciar documentos em um sistema de gestão documental	Controlar, arquivar e manter documentos dentro de um sistema de gestão
Preservar os documentos selecionados	Garantir a preservação de longo prazo dos documentos escolhidos para manutenção permanente

Fonte: Elaborado pela autora com base em Duranti e Rogers (2022)

Para enfrentar esses desafios e consolidar métodos periciais e arquivísticos, desenvolveu-se a disciplina *Digital Records Forensics* (DRF), abordada a seguir. Entre abril de 2008 a abril de 2011, pesquisadores canadenses, em colaboração com a Escola de Biblioteconomia, Arquivologia e Estudos da Informação (SLAIS) da Universidade da Colúmbia Britânica, a Faculdade de Direito da UBC e a Divisão de Perícia Forense Computacional do Departamento de Polícia de Vancouver, iniciaram o desenvolvimento de uma nova disciplina: Digital Records Forensics, traduzindo para o português, Perícia de Documentos Digitais (DRF Project, online).

O Projeto tinha como objetivo:

- desenvolver conceitos e métodos que permitam que os profissionais de gestão de documentos, arquivistas, do direito, do judiciário e aplicação da lei reconheçam documentos entre todos os tipos de objetos digitais produzidos por tecnologias digitais, uma vez que tenham sido removidos do sistema original;
- desenvolver conceitos e métodos para determinar a autenticidade de documentos que não estão mais no sistema original e/ou no formato original;
- desenvolver métodos para manter documentos adquiridos em cenas de crime ou criados pela polícia para investigar crimes a longo prazo, de modo que sua autenticidade não seja questionada; e
- desenvolver o conteúdo teórico e metodológico de uma nova disciplina, denominada Perícia de Documentos Digitais, resultante da integração da Diplomática Arquivística, da Computação Forense e do Direito Probatório com os resultados apresentados pelo projeto (DRF Project, online, tradução nossa).

O modelo *Digital Records Forensics* (DRF) combina fundamentos arquivísticos com procedimentos da perícia digital (Figura 1), assegurando que os registros sejam coletados, geridos e preservados de forma confiável ao longo de todo o ciclo de vida, considerando seu uso como evidência e seu enquadramento jurídico. Trata-se de um modelo que promove a integração entre arquivologia e forense digital, garantindo autenticidade, integridade e confiabilidade aos documentos digitais.

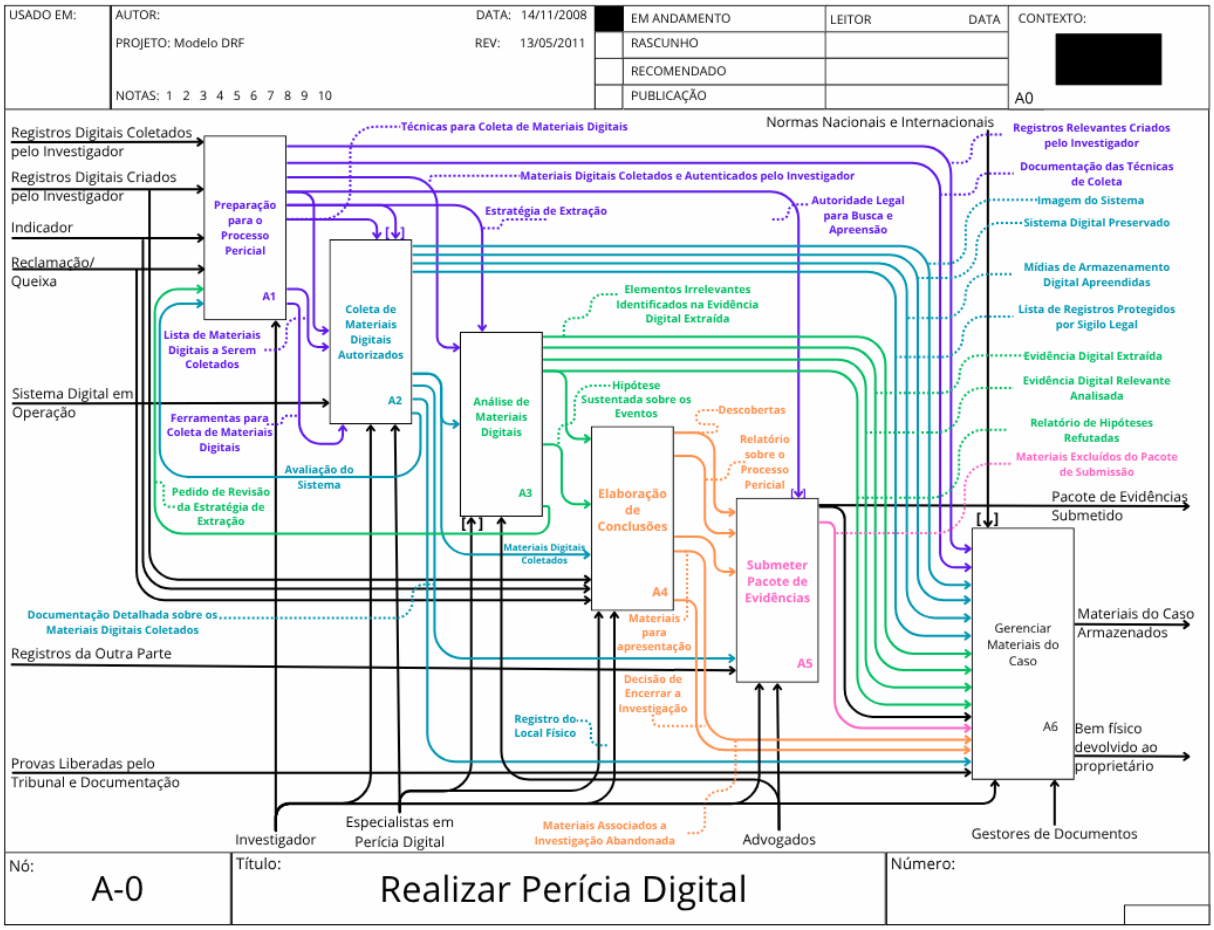
O DRF enfatiza a identificação e a preservação de registros digitais enquanto documentos arquivísticos, priorizando práticas que sustentem sua autenticidade e fidedignidade ao longo do tempo. Sua abordagem conjuga princípios diplomáticos com técnicas forenses, abrangendo tanto a captura inicial de evidências (como imagens bit a bit e geração de *hashes*) quanto o registro de informações contextuais sobre criação, manutenção, políticas de retenção e eventuais mudanças de formato. Esses elementos possibilitam a reprodução e a validação futura dos documentos, mesmo em ambientes tecnológicos distintos do original.

Por sua vez, a *Digital Forensics* concentra-se primordialmente nas técnicas e procedimentos utilizados para a descoberta, análise e apresentação de evidências digitais relacionadas a incidentes, crimes ou litígios. Seu foco recai sobre a

integridade, a cadeia de custódia e a admissibilidade jurídica, envolvendo atividades como atribuição temporal, recuperação de dados apagados e correlação de artefatos para demonstrar eventos e responsabilidades. Trata-se de uma área essencialmente técnica, fundamentada em ferramentas e metodologias específicas de investigação.

Já a Gestão Arquivística dedica-se à administração contínua dos documentos ao longo de seu ciclo de vida, estabelecendo políticas de classificação, retenção, acesso e preservação. Enquanto a *Digital Forensics* se volta à produção da prova imediata e o DRF articula procedimentos para assegurar a preservação de evidências como documentos arquivísticos, a gestão arquivística fornece o arcabouço institucional e normativo que possibilita que registros sejam produzidos, organizados e mantidos de forma íntegra, com valor administrativo, histórico e probatório.

Figura 1 – Realizar Perícia Digital A0

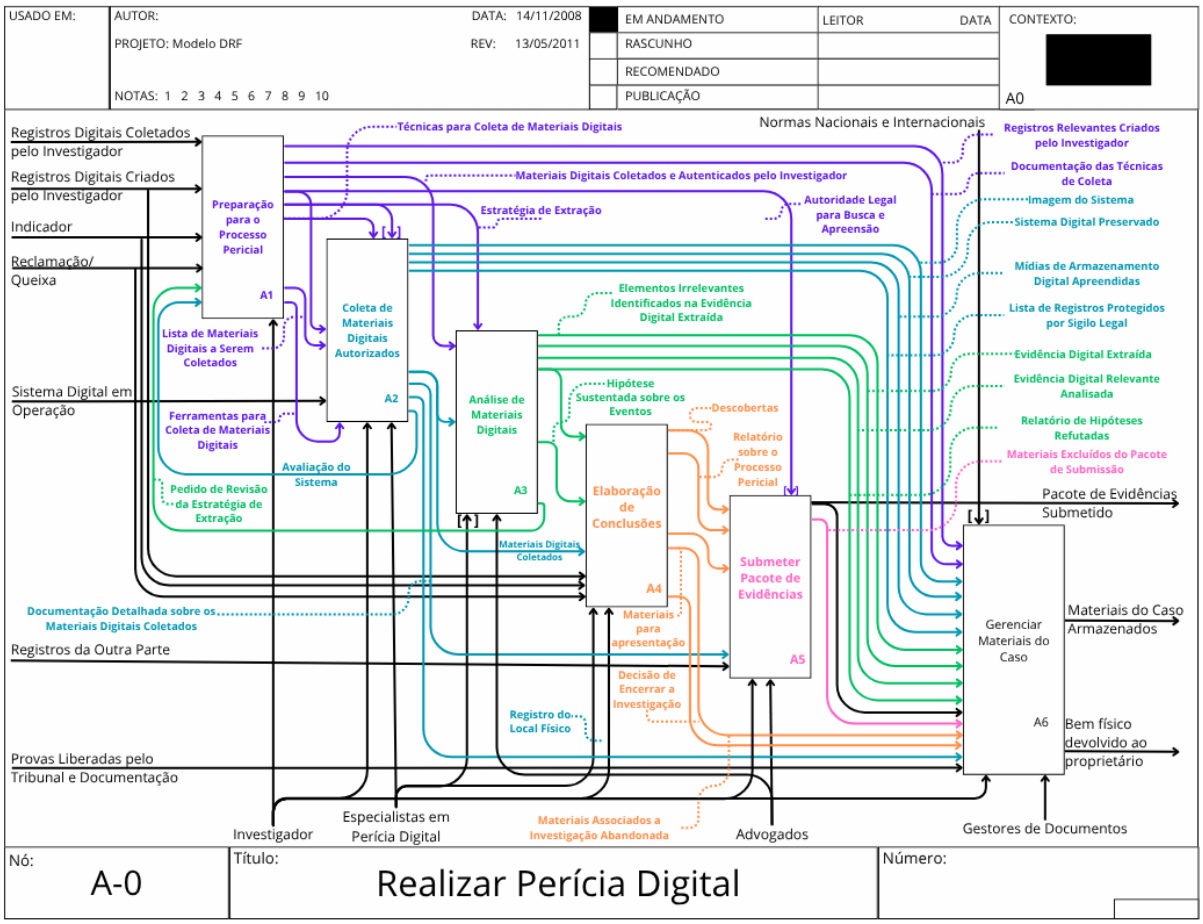


Fonte: Adaptado de Duranti e Rogers (2013, online, p. 8)

A Figura 2 ilustra a gestão de documentos dentro de um sistema de preservação permanente, mostrando como a Cadeia de Preservação (CoP) garante a

manutenção da autenticidade, integridade e confiabilidade dos registros digitais ao longo do tempo. O modelo evidencia a necessidade de integração entre práticas arquivísticas e procedimentos periciais, permitindo que os documentos digitais possam ser utilizados como evidência confiável em contextos judiciais e administrativos.

Figura 2 – Gerenciar Documento em um Sistema de Preservação Permanente (CoP)



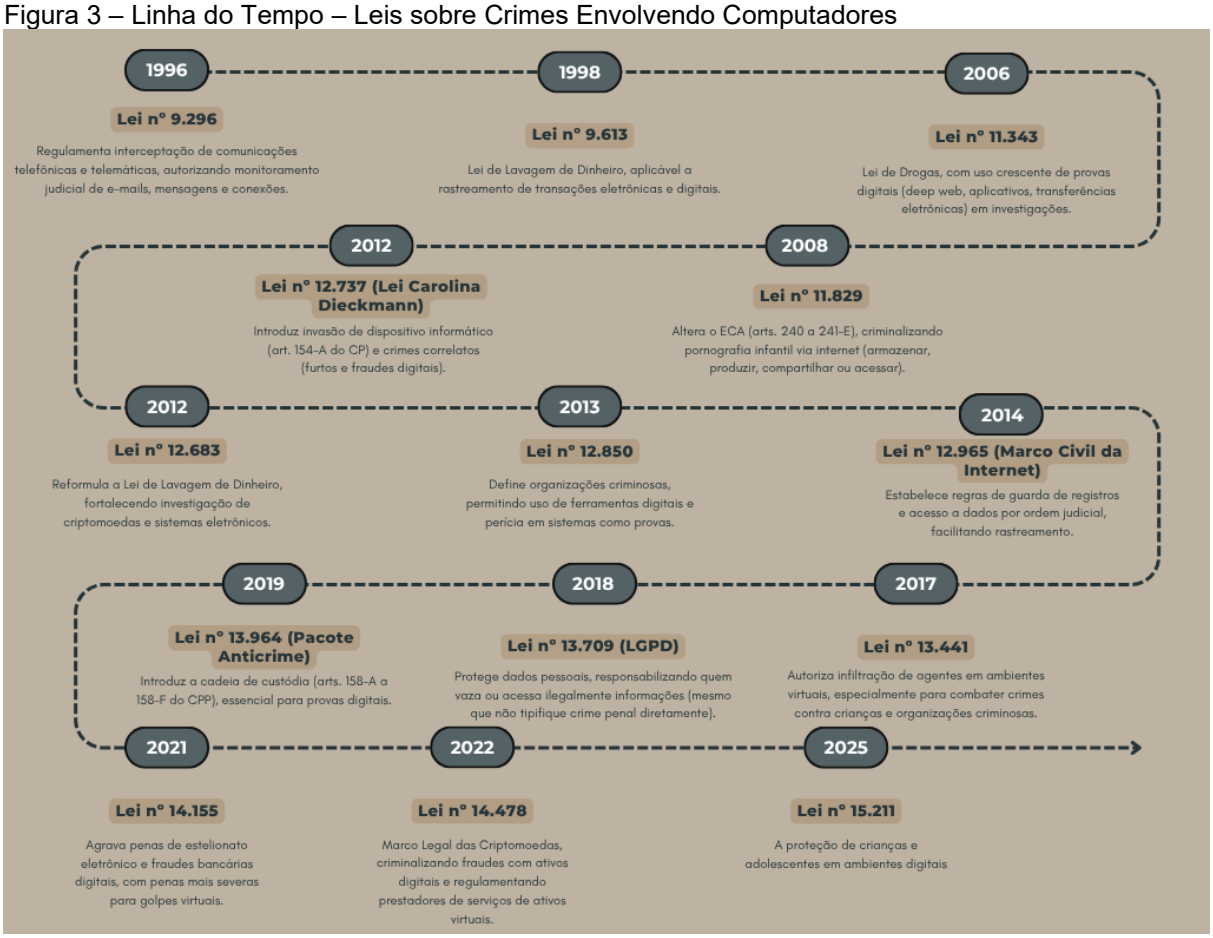
Fonte: Adaptado de Duranti e Rogers (2013, online, p. 9)

A integração ilustrada nas Figuras 1 e 2 demonstra que a gestão adequada de documentos digitais exige não apenas procedimentos periciais rigorosos, mas também práticas arquivísticas que assegurem a preservação e autenticidade ao longo do tempo. Assim, a adoção de modelos como o *Digital Records Forensics* (DRF) e a Cadeia de Preservação (CoP) constitui um passo fundamental para enfrentar os desafios impostos pelo ambiente digital, preparando o terreno para a análise da legislação brasileira e das políticas públicas voltadas à proteção de dados e combate a crimes cibernéticos.

3 LEGISLAÇÃO BRASILEIRA SOBRE CRIMES DIGITAIS

A legislação brasileira (Figura 3) voltada para crimes digitais e provas eletrônicas é relativamente recente e ainda em processo de amadurecimento. O primeiro marco relevante foi a Lei nº 9.296/1996, que regulamentou a interceptação de comunicações telefônicas e telemáticas. Nos anos 2000, surgiram normas pontuais, como a Lei nº 11.829/2008, que ampliou o Estatuto da Criança e do Adolescente para criminalizar a pornografia infantil online.

Figura 3 – Linha do Tempo – Leis sobre Crimes Envolvendo Computadores



Fonte: Elaborado pela autora.

Somente a partir dos anos 2000, o país passou a consolidar um marco normativo mais abrangente. A Lei nº 12.737/2012 (conhecida como Lei Carolina Dieckmann) criminalizou a invasão de dispositivos informáticos. Em seguida, o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu direitos e deveres para usuários e provedores, incluindo a guarda de registros de conexão e acesso. A Lei nº

13.709/2018 (LGPD) trouxe a proteção de dados pessoais ao centro do debate, enquanto a Lei nº 14.155/2021 tipificou o estelionato eletrônico.

Mais recentemente, a Lei nº 14.478/2022 criou o marco regulatório dos criptoativos, prevendo regras para prestadores de serviços de ativos virtuais. Em 2025, foi sancionada a Lei nº 15.211/2025 (ECA Digital), que estabelece medidas específicas de proteção a crianças e adolescentes no ambiente digital, impondo obrigações às plataformas e serviços online.

Quadro 2 - Leis e Crimes com Uso de Computadores

Lei	Assunto	Pena	Exemplo
Lei 9.296/1996	Interceptação de comunicações telefônicas e telemáticas (autorizada)	Depende do crime investigado	Gravação judicial de mensagens e e-mails para investigação de organização criminosa.
Lei 11.829/2008 (ECA)	Arts. 240 a 241-E – Pornografia infantil online	1 a 8 anos de prisão	Armazenar, compartilhar ou produzir conteúdo pornográfico infantil na internet.
Lei 12.737/2012 (Lei Carolina Dieckmann)	Art. 154-A – Invasão de dispositivo informático	1 a 4 anos de prisão + multa	Hacker invade e-mails de empresa para roubar dados ou dinheiro.
Lei 12.965/2014 (Marco Civil da Internet)	Guarda de registros e fornecimento de dados	Não define pena criminal direta	Provedor é obrigado a guardar logs para rastrear autor de ataque hacker.
Lei 13.709/2018 (LGPD)	Proteção de dados pessoais	Sanções administrativas (multas, restrições)	Empresa exposta por vazamento de dados de clientes.
Lei 14.155/2021	Estelionato eletrônico	4 a 8 anos de prisão + multa	Golpes de PIX, phishing e clonagem de WhatsApp para obter vantagem financeira.
Lei 14.478/2022	Crimes com ativos virtuais (fraudes e pirâmides)	4 a 8 anos de prisão + multa	Plataforma de criptomoeda fraudulenta que engana investidores.
Lei 15.211/2025 (ECA Digital)	Crimes e responsabilidades envolvendo crianças e adolescentes no ambiente digital	Variável conforme o crime	Plataformas obrigadas a remover conteúdos ilícitos e proteger menores contra exploração online.

Fonte: Elaborado pela autora.

Ainda em tramitação, o Projeto de Lei nº 4939/2020, busca regulamentar a coleta, a cadeia de custódia e a admissibilidade da prova digital no processo penal, apontando para um próximo avanço normativo.

Do ponto de vista pericial e arquivístico, a legislação impacta diretamente a forma de coletar, preservar e validar a prova digital. O Quadro 3 apresenta a aplicação

prática da legislação brasileira sobre crimes digitais no contexto pericial, incluindo exame de corpo de delito, cadeia de custódia e elaboração de laudos.

Quadro 3 – Aplicação a Crimes Envolvendo Computadores

Artigo CPP	Tema	Aplicação em Crimes com Computador
158	Exame de corpo de delito obrigatório	Análise de dispositivos, logs, softwares e registros digitais para comprovar crime mesmo com confissão.
158-A a 158-F	Cadeia de custódia	Documentação e preservação de HDs, servidores, mídias e nuvens para garantir integridade da prova.
159	Perito oficial e assistentes técnicos	Perícia feita por profissional especializado com nível superior; advogados podem indicar assistentes para acompanhar a análise.
160 a 170	Laudo pericial e procedimentos	Descrição de métodos forenses (cópia bit a bit, hashes, logs) para análise de sistemas e dispositivos.
171 a 184	Validade da prova e novas perícias	Possibilidade de contestar laudos, pedir perícia complementar ou revisar metodologia empregada.

Fonte: Elaborado pela autora.

Essa trajetória evidencia como o ordenamento jurídico brasileiro passou, ao longo de quase três décadas, de iniciativas fragmentadas para um arcabouço mais estruturado, ainda em expansão. A legislação não apenas tipifica crimes digitais, mas também estabelece diretrizes fundamentais para a prática pericial e a preservação da prova digital, conectando-se aos princípios de autenticidade, fidedignidade e integridade.

4 CONTEXTO TECNOLÓGICO E CIBERSEGURANÇA

Ao analisar o uso da palavra informação apresentado por Buckland – mais precisamente informação-como-coisa – “voltado para o que seria a representação da informação-como-conhecimento, ou seja, a maneira de dar tangibilidade ao que é intangível”, Rondinelli chega à conclusão que:

> É, pois, com base nessa noção de informação **como evidência**, isto é, como coisas por meio das quais nos tornamos informados, que passamos a apresentar o que Buckland identifica como quatro tipos de informação-como-coisa: dados, textos e **documentos**, objetos e, por último, eventos (Rondinelli, 2013, p. 39, grifo nosso).

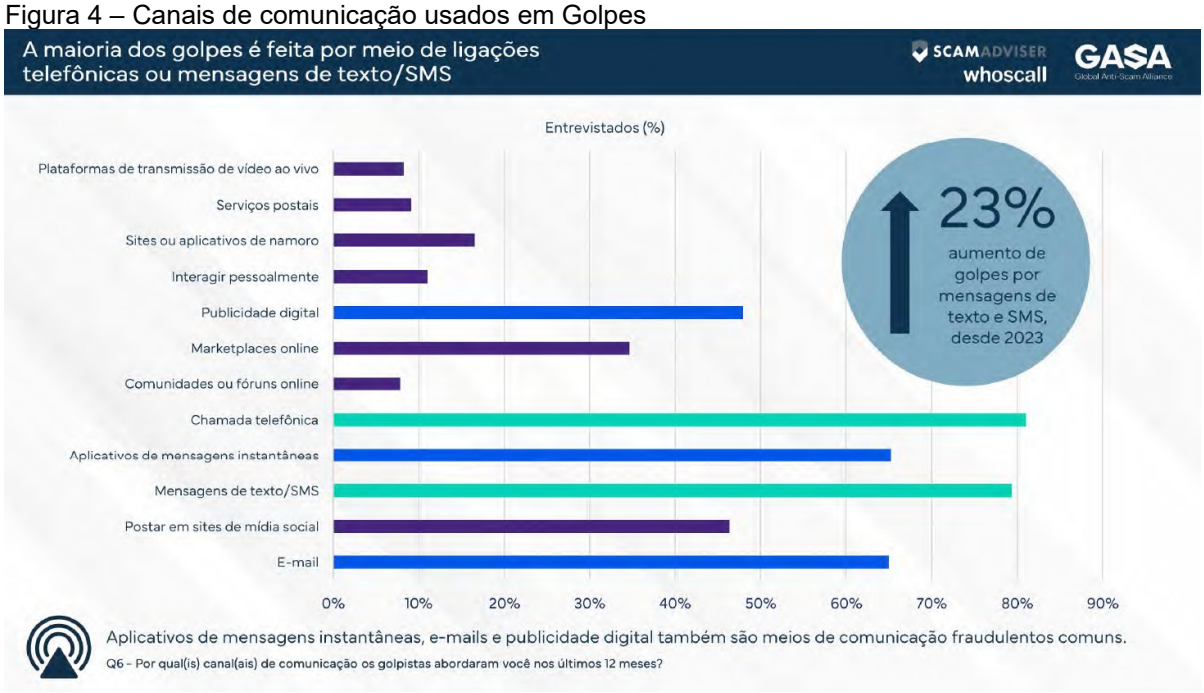
No contexto tecnológico atual, cada um desses tipos de informação-como-coisa pode ser gerado, armazenado ou transmitido por diferentes dispositivos, sistemas e redes, incluindo computadores, smartphones, servidores corporativos e serviços de nuvem. A variedade de formatos digitais e a multiplicidade de plataformas aumentam a complexidade da coleta e preservação de evidências digitais, exigindo que profissionais de perícia digital considerem não apenas o conteúdo, mas também metadados, logs e rastros deixados nos sistemas (Casey, 2011). Esse ecossistema amplia as possibilidades de produção, transmissão e armazenamento da informação, que circula em diferentes formatos e, cada vez mais, é gerida em plataformas de computação em nuvem. Embora essa infraestrutura ofereça escalabilidade e acesso remoto, também traz desafios técnicos e jurídicos relacionados à jurisdição, à segurança e à preservação de longo prazo.

Ao mesmo tempo, as mesmas tecnologias que impulsionam a comunicação e a gestão informacional expõem novas vulnerabilidades. Entre as mais recorrentes estão a manipulação de arquivos digitais, a invasão de sistemas, as falhas em logs e registros de auditoria, os ataques de *ransomware* e as adulterações audiovisuais como os *deepfakes*. Casos recentes ilustram a gravidade da situação: o Brasil figura entre os países mais atacados do mundo, com 1.379 golpes por minuto (CNN Brasil, 2025), e o maior vazamento de dados já registrado expôs 16 bilhões de senhas em escala global (Forbes Brasil, 2025).

Organizações como a Global Anti-Scam Alliance (GASA) têm destacado a importância de campanhas de conscientização e compartilhamento de informações sobre golpes digitais, reforçando a necessidade de educação digital para a sociedade. Em 2024, o relatório a respeito de golpes digitais, realizados através de diversos canais de comunicação (Figura 4) no Brasil, traz a informação que:

> Após crescentes esforços de conscientização, 62% dos brasileiros relataram confiança em sua capacidade de reconhecer golpes, um aumento de 5% em relação ao ano passado. No entanto, os golpes continuam difundidos, com 94% dos entrevistados tendo sido alvo de golpes pelo menos uma vez por mês - um aumento de 9% em comparação a 2023. Além disso, 67% dos brasileiros relataram ter sofrido mais tentativas de golpes no ano passado, indicando um aumento significativo na atividade de golpes, enquanto apenas 11% relataram uma redução (Gasa, 2024, p. 1).

Figura 4 – Canais de comunicação usados em Golpes



Fonte: Gasa (2024, p. 10)

No Brasil, iniciativas institucionais, como as desenvolvidas pelo Ministério Público de Minas Gerais (MPMG), buscam combater crimes cibernéticos por meio de programas de fiscalização, análise pericial de dispositivos e sistemas digitais e orientação à população sobre prevenção de fraudes online. “O Projeto Chegando Junto nasceu, com a visão de que era preciso fazer com que o Ministério Público também ocupasse o espaço digital com a mesma desenvoltura dos criminosos[...]” (Fernandes *et al*., 2024, tradução nossa). Além disso, “Conselho Nacional do Ministério Público (CNMP), que tem dado mais atenção ao tema, destacando em eventos nacionais a importância de potencializar ações para melhor prevenir e combater golpes” (GASA, 2024, p. 3).

> O Ministério Público do Estado de Minas Gerais foi o primeiro no Brasil a estabelecer uma unidade especializada para combater crimes cibernéticos em 2008, que desde então evoluiu para a estrutura atual de uma Força-Tarefa Especializada (GAECIBER). Atualmente, o GAECIBER conduz investigações e move ações penais contra os responsáveis por uma ampla gama de golpes, combinando expertise avançada em inteligência, tecnologia e direito (Gasa, 2024, p.4).

Nesse cenário, a cibersegurança desempenha papel central. Boas práticas, como o uso de criptografia, a realização de backups periódicos, a manutenção de logs confiáveis, a aplicação de autenticação multifator e o monitoramento contínuo, são

medidas essenciais para reduzir riscos. Contudo, a proteção da informação não se restringe ao campo técnico: depende igualmente de normas jurídicas e princípios arquivísticos. No Brasil, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelecem parâmetros de responsabilidade, privacidade e segurança.

5 CONSIDERAÇÕES FINAIS

O presente estudo evidencia que a prática da perícia digital não pode se restringir exclusivamente à tecnologia: é fundamental que os profissionais incorporem conceitos da teoria arquivística, reconhecendo que o documento digital, assim como os documentos físicos, possui valor probatório, histórico e social. A compreensão das categorias arquivísticas, da classificação de objetos digitais e da preservação de evidências digitais amplia a capacidade dos peritos de organizar, interpretar e proteger os dados de forma sistemática e confiável.

Além disso, a rápida evolução tecnológica impõe a necessidade de atualização contínua dos profissionais arquivistas e peritos digitais. Novas ferramentas, sistemas e técnicas de análise forense exigem que os especialistas estejam aptos a lidar com formatos diversos, plataformas de armazenamento em nuvem, dispositivos móveis e técnicas de manipulação digital, garantindo que a produção e a coleta de evidências mantenham rigor científico e validade jurídica.

O estudo também reforça o papel social das instituições públicas no combate a crimes cibernéticos e na promoção da segurança digital. O desenvolvimento de políticas públicas, programas de fiscalização e iniciativas educativas contribui para proteger a sociedade, aumentar a conscientização sobre golpes e fraudes digitais, e fortalecer a confiança nas instituições. Projetos como o “Chegando Junto” demonstram que ações coordenadas entre órgãos públicos, especialistas e organizações internacionais podem criar impacto significativo na prevenção de crimes digitais.

Este estudo é de natureza conceitual e exploratória, baseado em revisão da literatura, análise de projetos internacionais e interpretação normativa. Não realizou investigação empírica nem aplicação prática do DRF/CoP em instituições brasileiras; tampouco testou ferramentas forenses em cenários controlados. Essas limitações

reduzem a generalizabilidade empírica das conclusões e indicam a necessidade de estudos complementares que validem operacionalmente as propostas aqui discutidas.

Recomenda-se a realização de pesquisas empíricas para avaliar a aplicabilidade do modelo DRF/CoP em instituições públicas brasileiras (ex.: tribunais, ministérios públicos e arquivos estaduais), incluindo estudos de caso que analisem impactos sobre a fidedignidade probatória. Investigações sobre o papel de tecnologias distribuídas (blockchain) na preservação de evidências digitais e estudos específicos sobre o uso e detecção de Inteligência Artificial (deepfakes; machine learning adversarial) na criação e identificação de fraudes digitais são igualmente prioritários. Por fim, são sugeridos experimentos comparativos de ferramentas de preservação e de análise forense para estabelecer recomendações práticas de adoção institucional.

Em síntese, a integração entre teoria arquivística, perícia digital e tecnologia evidencia a necessidade de uma abordagem interdisciplinar, na qual o conhecimento técnico, a atualização profissional e a atuação institucional caminhem de forma articulada. Esse alinhamento é essencial não apenas para a eficiência operacional na coleta e preservação de evidências digitais, mas também para o fortalecimento do papel social das instituições e a proteção da sociedade frente às novas ameaças tecnológicas.

Destaca-se que a Cadeia de Custódia (CoC) é um instrumento legal e processual essencial para comprovar a guarda e integridade imediata da evidência, enquanto a Cadeia de Preservação (CoP) atua como complemento técnico-arquivístico responsável por registrar práticas, políticas, metadados e transformações ao longo do tempo, sustentando a autenticidade e a fidedignidade de documentos digitais em horizontes temporais longos. A insuficiência em implementar a CoP pode comprometer a fidedignidade, mesmo quando a CoC foi observada, pois a prova pode perder informações contextuais e de preservação que tornam difícil a validação em momentos futuros.

REFERÊNCIAS

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Dispõe sobre a interceptação de comunicações telefônicas e telemáticas.

BRASIL. **Lei nº 11.829, de 24 de dezembro de 2008**. Estatuto da Criança e do Adolescente – pornografia infantil online.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Cria tipo penal para invasão de dispositivos informáticos (Lei Carolina Dieckmann).

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD).

BRASIL. **Lei nº 14.155, de 29 de maio de 2021**. Tipificação do estelionato eletrônico.

BRASIL. **Lei nº 14.478, de 27 de agosto de 2022**. Criptoativos: crimes e regras para prestadores de serviços.

BRASIL. **Lei nº 15.211, de 2025**. ECA Digital: proteção de crianças e adolescentes no ambiente digital.

BRASIL. **Projeto de Lei nº 4.939, de 2020**. Regulamenta coleta, cadeia de custódia e admissibilidade da prova digital no processo penal.

CASEY, E. **Digital evidence and computer crime**: forensic science, computers, and the internet. 3. ed. Academic Press, 2011.

DRF PROJECT. **Digital Records Forensics Project (2008-2011).** Disponível em: http://www.digitalrecordsforensics.org/index.cfm. Acesso em: 22 set. 2025.

DURANTI, L. Reliability and authenticity: the concepts and their implications. **Archivaria**, v. 39, p. 5–10, 1995.

DURANTI, L.; ROGERS, C. **Memory forensics**: integrating digital forensics with archival science for trusting records and data. 2013. p. 8-9. Disponível em: http://www.digitalrecordsforensics.org/drf_term_db.cfm. Acesso em: 1 out. 2025.

EASTWOOD, T. Reconsidering archival authenticity: Concepts and practices. **Arquivo & Administração**, Rio de Janeiro, v. 12, n. 2, p. 15-27, jul./dez. 2013. Tradução de Sérgio Conde de Albite Silva. Publicado originalmente em Archivaria, v. 37, p. 122-130, primavera 1994.

FERNANDES, R. H. *et al.* **Project chegando junto**: boosting scam prevention in Brazil. Global Anti-Scam Alliance – GASA, 2024. Disponível em: https://www.gasa.org/post/project-chegando-junto-boosting-scam-prevention-in-brazil. Acesso em: 2 out. 2025.

GLOBAL ANTI-SCAM ALLIANCE (GASA). **Golpes digitais no Brasil** – 2024. Haia: GASA, 2024. Disponível em: https://gasa.org. Acesso em: 2 out. 2025

INTERPARES TRUST. **Building trust in the online environment**, 2019. Disponível em: http://interparestrust.org. Acesso em: 1 out. 2025.

LUZ, C. S.; FLORES, D. **Cadeia de custódia e de preservação**: autenticidade nas plataformas de gestão e preservação de documentos arquivísticos. 2013. Disponível

em: https://www.academia.edu/34470671/Cadeia_de_custódia_e_de_preservação_autenticidade_nas_plataformas_de_gestão_e_preservação_de_documentos_arquivísticos. Acesso em: 1 out. 2025.

ROGERS, C. Forense Digital e a autenticidade dos documentos arquivísticos digitais. **Revista Brasileira de Preservação Digital**, Campinas, SP, v. 2, e021002, 2021. [Transcrição da palestra na live do IBICT]

RONDINELLI, R. C. **Documento arquivístico digital**: desafios da diplomática contemporânea. Cultura Acadêmica, 2013.

RUBIN, F. Das provas em espécie: da prova documental à inspeção judicial. **JusBrasil**, 16 set. 2013. Disponível em: https://www.jusbrasil.com.br/artigos/das-provas-em-especie-da-prova-documental-a-inspecao-judicial/121943629. Acesso em: 12 dez. 2025.