BLOG · TECNOLOGIA & AUTENTICIDADE

O que é C2PA e por que a Adobe, Microsoft e Google estão apostando nisso

Por **Comitê de Tecnologia e Compliance da Provvi**

Toda vez que uma imagem circula na internet sem qualquer indicação de sua origem, uma pergunta fica sem resposta: isso é real? Foi editado? Quando e onde foi capturado? Por muito tempo, essa pergunta não tinha resposta técnica confiável. O C2PA veio para mudar isso.

Nos últimos três anos, o padrão ganhou a adesão de algumas das maiores empresas de tecnologia do mundo. Adobe, Microsoft, Google, Sony, Nikon, Leica, Intel e mais de 6.000 organizações ao redor do globo já adotaram ou estão implementando o C2PA em seus produtos. Não se trata de uma tendência passageira: é a resposta da indústria a uma crise crescente de confiança no conteúdo digital.

O problema que o C2PA resolve

Vivemos em um momento em que a manipulação de imagens se tornou acessível a qualquer pessoa com um smartphone. Ferramentas de inteligência artificial geram fotos realistas de pessoas que nunca existiram, eventos que nunca aconteceram, documentos que nunca foram assinados. O deepfake, que até poucos anos atrás exigia conhecimento técnico avançado, hoje é produzido em segundos por aplicativos gratuitos.

O impacto disso vai muito além das fake news políticas. No setor de seguros, imagens forjadas sustentam fraudes milionárias. Em processos judiciais, fotos adulteradas são apresentadas como provas. Em auditorias corporativas, registros visuais sem rastreabilidade comprometem a integridade das operações. A pergunta "isso é real?" deixou de ser filosófica e se tornou um problema prático e financeiro.

O que é, afinal, o C2PA

C2PA é a sigla para *Coalition for Content Provenance and Authenticity* — Coalizão para Proveniência e Autenticidade de Conteúdo. É um padrão técnico aberto, desenvolvido colaborativamente por empresas de tecnologia, fabricantes de câmeras, agências de notícias e plataformas digitais, com um objetivo central: criar um sistema verificável que registre a origem e o histórico de qualquer arquivo digital.

O padrão foi fundado em 2021 por Adobe, Microsoft, Arm, Intel e Truepic, unindo dois projetos anteriores: a **Content Authenticity Initiative (CAI)**, liderada pela Adobe, e o **Project Origin**, co-liderado por Microsoft e BBC, voltado ao combate à desinformação no ecossistema de notícias digitais.

O mecanismo central do C2PA é o que a coalizão chama de **Content Credentials** — uma espécie de "rótulo nutricional" para arquivos digitais. Assim como um rótulo de alimento informa ingredientes, origem e validade, os Content Credentials informam onde o conteúdo foi criado, com qual dispositivo, quando, se foi editado e por quem.

Como funciona tecnicamente — sem complicar

Quando uma câmera, um aplicativo ou um software compatível com C2PA captura ou processa uma imagem, ele cria um **manifesto** — um bloco de dados embutido no próprio arquivo. Esse manifesto contém:

- A impressão digital (hash) do conteúdo original, que muda se qualquer pixel for alterado
- Metadados de origem: dispositivo, localização, data e hora
- O histórico de edições aplicadas ao arquivo
- Uma assinatura criptográfica que vincula tudo a uma identidade verificável

A assinatura criptográfica é a parte mais importante. Ela funciona como um lacre: se qualquer dado do manifesto for alterado após a assinatura, a verificação falha. É matematicamente impossível modificar o conteúdo sem que a adulteração seja detectada.

> *"Content Credentials funcionam como um rótulo nutricional para conteúdo digital, disponível para qualquer pessoa acessar, a qualquer hora." — Coalition for Content Provenance and Authenticity (C2PA)*

Por que Adobe, Microsoft e Google estão apostando nisso

A resposta curta: porque o problema que o C2PA resolve ameaça o núcleo do negócio dessas empresas.

A **Adobe** vende ferramentas criativas. Se ninguém mais confia em imagens digitais, o valor do trabalho de designers, fotógrafos e videomakers se evapora. A empresa tem interesse direto em que imagens autênticas sejam distinguíveis das manipuladas.

A **Microsoft** co-fundou o Project Origin porque a desinformação afeta a confiança nas plataformas de notícias que monetiza. O Azure, sua plataforma de nuvem, é cada vez mais usado para processar e armazenar ativos digitais críticos — e clientes corporativos exigem rastreabilidade.

O **Google** enfrenta um desafio ainda mais agudo: seu motor de busca é o principal distribuidor de imagens na internet. Com a proliferação de deepfakes, a relevância do Google Imagens depende de conseguir diferenciar o real do sintético. A empresa já anunciou suporte a Content Credentials no Search.

Fabricantes de câmeras como **Sony, Nikon, Leica e Fujifilm** enxergam no C2PA uma forma de reafirmar o valor do hardware fotográfico profissional. Uma foto tirada com câmera certificada C2PA carrega uma prova de autenticidade que nenhuma imagem gerada por IA pode replicar.

O C2PA não é só para combate a deepfakes

Embora o debate público gire em torno de desinformação e IA generativa, as aplicações práticas vão muito além:

- **Seguros e vistorias:** imagens capturadas com C2PA são provas verificáveis de sinistros, laudos e inspeções de campo, eliminando disputas sobre adulteração.
- **Jornalismo e documentação:** agências de notícias como AP e Reuters já adotam o padrão para certificar fotos de guerra e eventos críticos.
- **Compliance e auditoria:** registros visuais de processos industriais, obras e inspeções ganham rastreabilidade completa.
- **Saúde:** imagens médicas com proveniência verificável reduzem disputas em laudos e processos judiciais.
- **Direito e prova digital:** evidências fotográficas com manifesto C2PA têm cadeia de custódia verificável independentemente.

O que acontece quando não há C2PA

Sem um padrão de proveniência, qualquer imagem é tecnicamente repudiável. Um advogado pode questionar a autenticidade de uma foto de sinistro. Uma seguradora pode negar um pagamento alegando manipulação. Um juiz pode desconsiderar uma evidência visual por falta de cadeia de custódia.

Esse não é um cenário hipotético. À medida que ferramentas de manipulação se tornam mais acessíveis, a contestação de evidências visuais se torna uma estratégia jurídica cada vez mais comum. Empresas que dependem de imagens como documentação operacional estão expostas a um risco que poucos percebem.

O padrão está maduro o suficiente para uso corporativo?

Sim. O C2PA publicou sua especificação técnica v1.0 em 2022 e a versão 2.0 chegou em 2024 com suporte expandido para vídeo e transmissões ao vivo. A biblioteca de referência (c2pa-rs) é open-source e disponível em Rust, Python, Node.js e C/C++.

Mais de 6.000 organizações já são membros da CAI. Câmeras Leica, Sony Alpha e Nikon Z6 III já assinam imagens com C2PA no momento da captura. O Adobe Lightroom preserva os Content Credentials durante a edição. O LinkedIn exibe selos de autenticidade em imagens verificadas. A adoção deixou de ser experimental e se tornou infraestrutura.

No Brasil, o padrão ganhou uma camada adicional de relevância com a combinação com a **ICP-Brasil** — a infraestrutura de chaves públicas do governo federal. Manifestos C2PA assinados com certificados ICP-Brasil têm validade jurídica reconhecida pelo ordenamento legal brasileiro, transformando autenticidade técnica em prova admissível.

Produzido por **Comitê de Tecnologia e Compliance da Provvi**