DIREITO & TI

ISSN 2447-1097 | Qualis A4

www.direitoeti.com.br

Vigilância algorítmica e adultização: o fenômeno do transbordamento de tutela

Algorithmic surveillance and adultization: the guardianship spillover phenomenon

Melhym Pereira Quemel[1]

Recebido em: 19.12.2025
Aprovado em: 10.06.2026

RESUMO

A pesquisa investiga o impacto da Lei nº 15.211/2025 na vigilância algorítmica e na adultização em ambientes virtuais. O estudo analisa o fenômeno do transbordamento de tutela, que ocorre quando mecanismos de controle desenhados para proteger vulneráveis incidem sobre a privacidade de adultos. O objetivo geral consiste em avaliar os riscos à validade da prova penal decorrentes dessa vigilância massiva e da automatização de reportes. Utiliza-se o método dedutivo e o estudo de caso comparado entre as jurisdições do Brasil e dos Estados Unidos. Os resultados demonstram que a recepção acrítica de relatórios de inteligência artificial rompe a cadeia de custódia e delega tacitamente o poder de polícia a entes privados, gerando insegurança jurídica. A pesquisa conclui com a proposição do protocolo de verificação preliminar, um standard de admissibilidade que converte a inteligência privada em evidência forense auditável. Tal mecanismo visa harmonizar a proteção integral da infância com as garantias do devido processo legal no Estado Democrático de Direito.

Palavras-chave: Adultização e Cibersegurança; Cadeia de Custódia; Protocolo de Verificação Preliminar; Prova Digital; Transbordamento de Tutela.

ABSTRACT

This research investigates the impact of Law No. 15.211/2025 on algorithmic surveillance and adultization in virtual environments. The study analyzes the guardianship spillover phenomenon, which occurs when control mechanisms designed to protect the vulnerable inadvertently encroach upon adult privacy. The main objective is to evaluate the risks to the validity of criminal evidence arising from mass surveillance and automated reporting. It employs the deductive method and a comparative case study between Brazilian and United States jurisdictions. Results demonstrate that the uncritical acceptance of artificial intelligence reports breaks the chain of custody and tacitly delegates police power to

[1] Mestre em Direito pela Universidade Estácio de Sá/RJ. Especialista em Advocacia Cível pela FMP/RS e Ciências Penais e Segurança Pública pelo Instituto Rogério Greco/MG. Advogado. Lattes: http://lattes.cnpq.br/4629884576807167; Orcid: https://orcid.org/0000-0003-3103-6754.

private entities, creating legal uncertainty. The study concludes by proposing the preliminary verification protocol, an admissibility standard that converts private intelligence into auditable forensic evidence. This mechanism aims to harmonize integral child protection with due process guarantees within the Democratic State of Law.

Keywords: Guardianship Spillover; Adultization and Cybersecurity; Chain of Custody; Digital Evidence; Preliminary Verification Protocol.

1 INTRODUÇÃO

A arquitetura da cibersegurança contemporânea atravessa uma mutação irreversível, impulsionada pelo imperativo ético e jurídico de combater a adultização precoce e a exploração sexual infantojuvenil em ambientes virtuais. Neste cenário de governança híbrida, onde o controle social opera majoritariamente em servidores privados, a promulgação do novo Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025) representa um marco civilizatório na proteção de vulneráveis. Ao impor deveres proativos de prevenção, detecção e reporte às plataformas digitais, o legislador brasileiro reconheceu que a proteção integral da infância exige, na atualidade, uma vigilância algorítmica ininterrupta e onipresente.

Contudo, a implementação tecnológica dessas salvaguardas revela um paradoxo situado na tensa intersecção entre o Direito Digital e o Processo Penal: para blindar a criança contra a violência, as plataformas impuseram, por via reflexa, uma vigilância que excede seu alvo original. Observa-se, assim, uma distorção nos vetores de controle parental e na calibragem dos algoritmos de direcionamento – temas centrais no debate sobre adultização –, pois as ferramentas criadas para filtrar o conteúdo nocivo à criança passaram a esquadrinhar a vida privada do adulto, criando uma zona cinzenta de monitoramento.

Todavia, essa nova arquitetura normativa engendra uma contradição sociológica e jurídica fundamental, diretamente vinculada ao fenômeno da adultização. Paradoxalmente, enquanto a sociedade e o legislador envidam esforços para frear a adultização precoce de crianças – protegendo-as da exposição a conteúdos e responsabilidades impróprias que geram ansiedade e hiperestimulação incompatíveis com a psique em formação –, o aparato tecnológico de vigilância responde com uma espécie

de 'infantilização da privacidade' do cidadão adulto. Sob a justificativa da proteção integral, o Estado e as plataformas passam a tutelar a intimidade de todos os usuários com o mesmo rigor paternalista e invasivo necessário à salvaguarda dos incapazes, gerando um efeito colateral sistêmico que merece escrutínio constitucional.

Este fenômeno, aqui conceituado como "Transbordamento de Tutela", ocorre quando ferramentas de monitoramento desenhadas para proteger crianças passam a incidir, silenciosa e sistematicamente, sobre a privacidade de adultos. Ao aderir aos termos de serviço de armazenamento em nuvem, o cidadão submete-se a uma varredura automatizada contínua que, embora legitimada moralmente pelo combate a crimes sexuais contra menores, acaba por redefinir os limites globais da privacidade e as fronteiras da persecução penal.

O problema de pesquisa que orienta este artigo reside na validade jurídica e epistêmica desse arranjo: a varredura massiva, justificada pela proteção da infância, pode servir de justa causa automática para a ação penal em crimes diversos, sem violar a vedação legal à vigilância indiscriminada e sem romper a cadeia de custódia da prova digital?

O debate acadêmico e jurisprudencial predominante tem enfrentado essa questão sob a ótica da doutrina da "busca privada" (*private search*), sustentando que a Quarta Emenda ou as garantias constitucionais brasileiras não se aplicariam a descobertas feitas por entes particulares sem intervenção estatal direta. Todavia, este estudo desafia tal premissa, argumentando que a imposição legal de deveres de monitoramento transforma as plataformas em agentes estatais por delegação, tornando obsoleta a distinção entre vigilância pública e privada.

A tese central a ser refutada é a de que o consentimento contratual do usuário ("Li e Aceito") equivale a uma renúncia irretratável à privacidade, capaz de validar uma devassa prospectiva em seus dados pessoais.

Nesse contexto, o objetivo geral deste trabalho é analisar os riscos à validade da prova penal decorrentes desse transbordamento de tutela, investigando se a arquitetura atual de recepção da prova digital fere o devido processo legal.

Especificamente, busca-se demonstrar o colapso da doutrina da busca privada diante da moderna Teoria do Mosaico, examinar a natureza da "serendipidade híbrida" – o encontro fortuito de provas por algoritmos não humanos – e desenhar um protocolo de segurança jurídica que mitigue nulidades processuais.

A hipótese central defendida é a de que o atual mecanismo de cooperação entre plataformas e Estado configura uma modalidade de prova desprovida de controles epistêmicos adequados. Operando sob uma espécie de "Constituição Privada", tais elementos probatórios, se recepcionados sem filtros rigorosos, violam a integridade da cadeia de custódia e geram um sistema de vigilância panóptica incompatível com o Estado Democrático de Direito.

A simples importação de relatórios de inteligência artificial, sem a interposição de um controle jurisdicional específico, cria um vácuo de garantias que, paradoxalmente, pode levar à anulação de investigações legítimas, frustrando a própria proteção da infância que se visa garantir.

Para a verificação desta hipótese, adota-se o método dedutivo, partindo das premissas constitucionais de proteção de dados e privacidade para a análise da nova legislação infraconstitucional. O procedimento metodológico inclui um estudo de caso comparado, utilizando precedentes da Suprema Corte dos Estados Unidos (*Carpenter v. United States*) como parâmetro hermenêutico para a interpretação da "expectativa de privacidade" em dados históricos, bem como a análise empírica de inquéritos policiais recentes no Brasil (como o caso do anestesista), onde a gênese probatória se deu exclusivamente por meio de reportes algorítmicos de *hash* desconhecido.

O artigo estrutura-se em três momentos lógicos para conduzir o leitor da teoria à proposição prática.

Inicialmente, analisa-se a natureza jurídica do reporte automatizado sob a nova lei, demonstrando a transmutação das plataformas em braços auxiliares do poder de polícia e a crise dos tratados de cooperação internacional (*Mutual Legal Assistance Treaties*).

Em seguida, demonstra-se a insuficiência das doutrinas tradicionais de validação da prova diante da capacidade de processamento de *Big Data* e da Teoria do Mosaico,

evidenciando como a acumulação de metadados permite uma reconstrução intrusiva da vida do indivíduo.

Por fim, propõe-se um inédito standard de admissibilidade: o Mandado de Verificação Preliminar (MVP). Este protocolo visa harmonizar a proteção integral do menor com as garantias do devido processo legal, estabelecendo etapas de validação estatal que transformam a inteligência algorítmica privada em evidência forense pública e auditável, superando a confiança cega nos sistemas automatizados.

Dessa forma, o presente estudo ultrapassa a mera análise legislativa para sustentar uma hipótese central: a de que a doutrina da 'busca privada' colapsou diante da vigilância algorítmica massiva. O objetivo, portanto, é demonstrar que a validade da prova penal na era do 'Transbordamento de Tutela' depende da superação da confiança cega nas plataformas e da implementação de um controle epistêmico rigoroso, aqui denominado Protocolo de Verificação Preliminar.

2 A "CONSTITUIÇÃO DIGITAL PRIVADA" E O BRAÇO DO ESTADO

A compreensão do fenômeno investigativo atual exige, preliminarmente, o desvelamento da natureza normativa das plataformas digitais. Não estamos diante de meros prestadores de serviço, mas do que Teubner (2016) classifica como "Regimes Privados Globais" (*Global Private Regimes*).

Na ausência de uma constituição global, corporações transnacionais produzem um direito autônomo (*Lex Mercatoria Digitalis*) que compete, e por vezes substitui, o direito estatal. Corroborando essa visão, Teixeira (2022) alerta que o Direito Digital contemporâneo enfrenta o desafio de regular entes que detêm o controle arquitetural da rede, muitas vezes impondo suas normas técnicas sobre as normas jurídicas.

2.1. Do contrato à delegação de Poder de Polícia: a opacidade da "caixa-preta"

Os Termos de Serviço (ToS) das plataformas digitais (GOOGLE, 2025) funcionam, na prática, como "Constituições Digitais Privadas", estabelecendo direitos,

deveres e penalidades (banimento, denúncia) à revelia do processo legislativo clássico. Contudo, a entrada em vigor da Lei nº 15.211/2025 altera a natureza jurídica dessa relação no Brasil. Ao estipular, em seu art. 27, que os fornecedores devem "remover e comunicar" conteúdos de exploração sexual às autoridades, o Estado brasileiro realiza uma delegação tácita de poder de polícia (BRASIL, 2025a).

Neste novo arranjo, opera-se o fenômeno descrito por Zuboff (2019) como a essência do "Capitalismo de Vigilância": a comoditização da privacidade, onde a experiência humana é extraída unilateralmente como matéria-prima comportamental.

O usuário, hipossuficiente diante da arquitetura de escolha da plataforma, "vende" sua blindagem constitucional (sigilo) em troca de armazenamento. A nova lei, embora vital para a proteção da infância, acentua essa assimetria ao obrigar o monitoramento massivo, criando uma simbiose perigosa entre o dever estatal e o lucro privado.

É nesse ponto que reside a fragilidade epistêmica do modelo. Um argumento recorrente na defesa dessa vigilância automatizada é a presunção de "boa-fé" das plataformas e a suposta neutralidade matemática dos algoritmos. Todavia, essa premissa carece de sustentação científica. Como alerta Pasquale (2015) em sua obra sobre a Black Box Society, os algoritmos não são oráculos imparciais, mas sim construtos empresariais protegidos por segredo industrial, cujos critérios de calibragem respondem a incentivos de mercado e não necessariamente ao devido processo legal.

No contexto da Lei nº 15.211/2025, essa opacidade gera o que a doutrina denomina de "viés de responsabilidade corporativa". Sob o temor de sanções pesadas por omissão no combate à exploração infantil, as plataformas ajustam seus filtros de hashing para uma sensibilidade extrema (super-notificação). O resultado estatístico é um aumento exponencial de falsos positivos – o cidadão comum que, por uma falha de contexto na leitura do bot, tem a sua privacidade devassada.

Juridicamente, o problema agrava-se pela impossibilidade de defesa. Se a "inteligência" que motivou a denúncia é uma caixa-preta proprietária, inacessível à defesa técnica sob o argumento de proteção da propriedade intelectual, aniquila-se o princípio do contraditório. A defesa não combate fatos, mas sim probabilidades matemáticas ocultas.

Portanto, aceitar a "serendipidade híbrida" baseada apenas na confiança cega na ferramenta é admitir uma prova de fé, incompatível com o standard probatório penal. Onde não há auditabilidade do código-fonte ou dos parâmetros de busca, não há prova, mas sim, na melhor das hipóteses, um indício não verificável que jamais poderia fundamentar, por si só, uma medida cautelar ou condenatória.

Essa assimetria contratual encontra sua raiz sociológica na própria crise da adultização. Conforme a sociedade falha em proteger a infância da exposição precoce a conteúdos adultos (adultização), o Estado e as Plataformas reagem com um protecionismo tecnológico que, paradoxalmente, infantiliza o cidadão adulto. Para proteger a criança da 'vida adulta' online, trata-se o adulto como um incapaz digital, cuja privacidade precisa ser tutelada e vigiada preventivamente por uma 'babá algorítmica'.

Isso agrava o fenômeno sociológico da 'Crise de Autoridade': ao retirar do adulto a autonomia sobre sua própria esfera privada, o algoritmo enfraquece a figura de referência necessária para guiar a criança, nivelando ambas as gerações sob a mesma vigilância paternalista das plataformas.

O 'Transbordamento de Tutela', portanto, é o preço pago pela incapacidade social de gerir as fronteiras da infância, resultando na imposição de uma 'minoridade cívica' a todos os usuários da rede, consolidando uma assimetria de poder onde as plataformas assumem a função de reguladoras do comportamento social, fenômeno intrínseco ao que se entende por capitalismo de vigilância (Zuboff, 2019).

2.2 O "bypass" jurisdicional e a crise do MLAT

A validação acrítica dessas provas no processo penal brasileiro revela outro problema estrutural: o contorno (*bypass*) dos tratados internacionais de cooperação. Conforme aponta Abreu (2018), o sistema de *Mutual Legal Assistance Treaties* (MLAT) é considerado moroso e ineficiente para a velocidade da era digital. Nesse sentido, Dias (2025) reforça que, embora a Convenção de Budapeste preveja mecanismos de agilização, a burocracia estatal ainda impulsiona a busca por vias alternativas de obtenção de dados.

Diante disso, autoridades investigativas brasileiras têm se valido dos reportes diretos do NCMEC (*National Center for Missing & Exploited Children*) ou das plataformas, ignorando o rito do MLAT. O relatório chega "pronto", contendo metadados, conteúdo e identificação, muitas vezes amparado apenas na legislação norte-americana (18 U.S. Code § 2258A) (Estados Unidos, 2024) e agora reforçado pelo art. 27 da Lei nº 15.211/2025 (Brasil, 2025a).

Todavia, Lima e Lima (2024) advertem que a admissibilidade desse reporte direto não é automática, exigindo cautela quanto à sua natureza unilateral. O risco desse *bypass* é a importação de provas sem a devida cadeia de custódia e sem o crivo da soberania nacional sobre a legalidade da obtenção. O Brasil corre o risco de viver o "pior dos dois mundos": submete-se à vigilância das leis estrangeiras (que permitem a varredura de dados) mas não aplica as garantias das leis estrangeiras (como a exigência de warrant para acesso a dados históricos, consolidada em Carpenter v. United States) (Estados Unidos, 2018).

Ao equiparar o "Li e Aceito" do contrato a uma autorização irretratável de busca e apreensão, o sistema jurídico opera uma ficção perigosa. O cidadão que armazena fotos de família na nuvem não possui a representação mental de que está autorizando uma "devassa policial terceirizada", capaz de montar um mosaico completo de sua vida privada sob o pretexto de buscar ilícitos específicos.

Estabelecido o cenário fático de vigilância delegada e *bypass* jurisdicional, torna-se imperioso analisar como as cortes constitucionais têm reagido a essa nova realidade. A ficção do consentimento contratual, sustentáculo da validade dessas provas, enfrenta agora o teste de fogo diante de doutrinas que já reconhecem a obsolescência da privacidade analógica frente ao poder reconstrutivo dos dados massivos.

3 O COLAPSO DA "PRIVATE SEARCH" E A TEORIA DO MOSAICO: LIÇÕES DO DIREITO COMPARADO

A validação jurídica dos relatórios de inteligência artificial (IA) no Brasil tem se sustentado, majoritariamente, na importação da doutrina norte-americana da Private

Search. Segundo este entendimento, originado em United States v. Jacobsen (Estados Unidos, 1984), a Quarta Emenda – que protege contra buscas irracionais – não se aplicaria a atos de particulares. Se uma Big Tech vasculha os arquivos de um usuário e entrega o crime "de bandeja" à polícia, não haveria ilicitude, pois o Estado não participou da quebra inicial da privacidade.

Todavia, essa importação ocorre com um delay hermenêutico perigoso. A jurisprudência da Suprema Corte dos Estados Unidos (SCOTUS) evoluiu substancialmente para reconhecer que, na era do Big Data, a distinção entre "público/privado" e "conteúdo/metadado" tornou-se obsoleta.

3.1 *Carpenter v. United States*: o fim da "doutrina do terceiro"

O ponto de inflexão ocorre no julgamento de *Carpenter v. United States* (Estados Unidos, 2018). O FBI, sem mandado judicial, obteve 127 dias de dados de geolocalização (CSLI) de um suspeito, argumentando que ele havia entregado voluntariamente essas informações à companhia telefônica (uma "terceira parte"). Pela clássica *Third-Party Doctrine*, quem entrega dados a terceiros perde a expectativa de privacidade.

A Suprema Corte, contudo, reverteu esse entendimento em uma decisão histórica (5-4). O *Chief Justice Roberts* asseverou que a posse de um celular é, hoje, "quase uma característica da anatomia humana", e não uma escolha voluntária genuína. O tribunal reconheceu que o acesso a dados históricos digitais confere ao Estado uma capacidade de "vigilância quase perfeita" (*near perfect surveillance*) e de "viagem no tempo" (time travel) para reconstruir a vida do cidadão (Estados Unidos, 2018).

A importação dessa ratio decidendi para o ordenamento brasileiro, mutatis mutandis, é estratégica para a interpretação da Lei nº 15.211/2025. Embora o Brasil não adote a *Third Party Doctrine* em sua integralidade, o fenômeno do 'transbordamento de tutela' cria um cenário fático análogo ao enfrentado em Carpenter: a impossibilidade de o sujeito exercer a cidadania digital sem gerar, compulsoriamente, metadados que revelam sua intimidade.

Portanto, a lição de Carpenter aqui não serve como precedente vinculante, mas como parâmetro hermenêutico de standards probatórios, indicando que a automação da vigilância – seja pelo GPS nos EUA, seja pelo algoritmo de proteção infantil no Brasil – altera a qualidade da violação à privacidade, exigindo, por simetria, um rigor maior no controle judicial da prova (warrants específicos) do que aquele aplicado à busca privada tradicional.

A *ratio decidendi* de Carpenter é clara: quando a vigilância é onipresente e inevitável, a "entrega a terceiros" (como o Google ou a Apple) não implica renúncia automática à privacidade. Se nos EUA exige-se *warrant* (mandado) baseado em *probable cause* até para saber onde o cidadão andou (metadados), com muito mais razão deve-se exigir controle judicial para saber o que ele armazena na nuvem (conteúdo).

A aplicação da *ratio decidendi* de Carpenter ao ordenamento brasileiro, contudo, enfrenta um hiato cultural e jurídico. Enquanto a Suprema Corte dos EUA evoluiu para exigir warrant (mandado) baseado em *probable cause* para dados históricos, o Brasil vive um 'atraso hermenêutico'. Nossos tribunais ainda operam sob a lógica analógica de que a entrega de dados a terceiros (provedores) enfraquece a expectativa de privacidade.

Portanto, a proposta deste artigo é de lege ferenda e de alteração de standard jurisprudencial: sustenta-se que a Lei nº 15.211/2025, ao tornar a vigilância compulsória, deveria atrair a proteção de Carpenter. Sem essa mudança de paradigma interpretativo – saindo da 'boa-fé' para a 'verificação auditável' –, o sistema brasileiro continuará validando provas que, na fonte original (EUA), já seriam consideradas inconstitucionais se obtidas diretamente pelo Estado sem mandado.

3.2 A Teoria do Mosaico e a vigilância algorítmica

Para compreender o 'Transbordamento de Tutela', é imperativo aplicar a *Mosaic Theory* (Teoria do Mosaico), extraída dos votos concorrentes da Suprema Corte dos EUA em *United States v. Jones* (Estados Unidos, 2012). A premissa epistêmica aqui supera a lógica da busca individualizada: a agregação sistêmica de dados inócuos pode revelar um perfil íntimo que nenhuma das partes isoladas exporia. Isso é devastador para a doutrina

da Private Search, pois transforma a moderação de conteúdo em uma vigilância panóptica (Estados Unidos, 2012).

Uma análise isolada de um único arquivo (um *hash match*) pode parecer uma intrusão mínima. Contudo, a Inteligência Artificial não analisa arquivos isolados; ela processa o conjunto informacional do usuário para inferir comportamentos.

Conforme leciona Kerr (2012), a agregação de dados ao longo do tempo cria um "mosaico" detalhado da vida de uma pessoa – suas preferências políticas, sexuais, religiosas e médicas – que jamais seria revelado por uma busca física tradicional.

No contexto do combate à adultização e ao CSAM, o algoritmo do Google não atua como um policial que olha uma foto específica; ele atua como uma rede de arrasto (*dragnet*). Para encontrar o ilícito infantil, ele precisa escanear a totalidade da vida digital do adulto.

Quando esse escaneamento encontra, por serendipidade, um crime diverso (como no caso do anestesista, a ser analisado), não houve um mero encontro fortuito de provas, mas a materialização de uma vigilância perpétua que, pela Teoria do Mosaico, constitui uma "busca" (*search*) constitucionalmente protegida, exigindo reserva de jurisdição.

3.3 A morte da voluntariedade: 18 U.S.C. § 2258A e a Lei nº 15.211/2025

O golpe final na tese de que as plataformas agem como "particulares benevolentes" reside na análise da legislação impositiva. Nos Estados Unidos, o *18 U.S. Code § 2258A* (Estados Unidos, 2024) impõe aos provedores o dever de reportar fatos e circunstâncias de crimes de exploração infantil, sob pena de multas severas. No Brasil, a recém-sancionada Lei nº 15.211/2025, em seu artigo 27, espelha essa obrigação, determinando a remoção e comunicação compulsória às autoridades (BRASIL, 2025a).

Juridicamente, isso transforma a natureza da ação. Quando a lei obriga o particular a vigiar e denunciar sob pena de sanção, o particular atua como *longa manus* do Estado (o "longo braço da lei"). A busca deixa de ser "privada" e torna-se uma "busca estatal delegada".

Ao ignorar essa transmutação, o sistema de justiça brasileiro caminha sobre gelo fino. Se o provedor age por mandato legal (Art. 27 da Lei 15.211/2025), sua ação está sujeita aos limites constitucionais do Art. 5º da CF/88. Validar essa prova como se fosse fruto de mera liberalidade contratual é criar um vácuo de garantias: o Estado investiga através da empresa para não precisar pedir mandado ao juiz. Essa manobra, embora eficiente no curto prazo, planta a semente de nulidades futuras que podem derrubar operações inteiras, prejudicando justamente a proteção da infância que se visa garantir.

Essa tensão teórica entre a eficiência da vigilância delegada e as garantias constitucionais deixa de ser uma abstração acadêmica quando confrontada com a realidade forense. Para demonstrar como o 'Transbordamento de Tutela' se materializa nos autos, passamos à análise de um caso paradigmático recente, onde a gênese algorítmica da prova desafiou os limites da serendipidade clássica.

4 O ANESTESISTA E O ALGORITMO: A SERENDIPIDADE HÍBRIDA NA PRÁTICA

A teoria do transbordamento de tutela ganha materialidade empírica na análise da praxis forense recente. Para ilustrar o fenômeno, seleciona-se como *leading case* o Inquérito Policial nº 947-01253-2022 (PCERJ), que tramitou perante a Justiça do Estado do Rio de Janeiro (2023). A escolha deste caso não se dá pela repercussão midiática dos fatos imputados, mas pela singularidade da gênese probatória, que desafia os paradigmas tradicionais da investigação criminal.

4.1 A gênese probatória: o "pacote" algorítmico e o arrasto contextual

Diferentemente da investigação policial clássica, iniciada pela linearidade da *notitia criminis* trazida pela vítima, a *persecutio criminis* no Caso A. E. O. C. (Processo nº 0800337-68.2023.8.19.0058) teve uma gênese derivada e tecnológica. O ponto de partida foi um *CyberTipline Report* gerado pelos algoritmos de detecção da Google, cujo alvo primário era a identificação de Material de Abuso Sexual Infantil (CSAM).

Trata-se do modelo de investigação criminal cibernética descrito por Wendt (2024), que rompe com a tradição inquisitorial cartorial, exigindo da autoridade policial a capacidade de interpretar reportes de inteligência que já nascem digitalizados e transnacionais. A plataforma, ao detectar arquivos contendo pornografia infantojuvenil – material cuja circulação perpetua a violência e distorce o desenvolvimento saudável da sexualidade na infância – na nuvem do usuário (Google Fotos), acionou o protocolo de reporte compulsório ao NCMEC, entidade que processa milhões de denúncias anualmente (National Center For Missing & Exploited Children, 2024).

Contudo – e aqui reside a materialidade do transbordamento de tutela –, o "pacote de evidências" (*evidence package*) gerado automaticamente pelo sistema e remetido às autoridades brasileiras (Polícia Federal e, posteriormente, DCAV/RJ) não continha apenas os arquivos ilícitos infantis. Valendo-se de critérios de preservação contextual, o algoritmo incluiu no reporte arquivos adjacentes encontrados no mesmo ambiente digital.

Conforme detalha Jorge (2025), a análise forense computacional depende da integridade dos códigos *hash* para individualizar arquivos conhecidos. No entanto, ao baixarem o material via protocolo seguro (SFTP) e analisarem o conteúdo em busca de vítimas infantis, os agentes da Polícia Civil do Rio de Janeiro depararam-se, por serendipidade, com vídeos documentando estupros de vulneráveis adultos (pacientes sedadas em ambiente hospitalar) (Rio de Janeiro, 2023).

Não houve uma busca intencional da IA por crimes contra adultos, mas um arrasto contextual (*contextual dragnet*). O sistema de proteção à infância funcionou como uma "chave mestra": a detecção do ilícito infantil legitimou a quebra do sigilo e o envio de um pacote de dados que expôs, sem mandado judicial específico prévio, a intimidade de terceiros adultos.

4.2 A Serendipidade Híbrida de Segundo Grau e a Opacidade da "Caixa-Preta"

O fenômeno observado neste caso representa uma sofisticação do conceito de encontro fortuito de provas. Na serendipidade clássica, a polícia busca um delito e encontra outro.

No caso A. E. O. C., a polícia não estava realizando uma busca ativa nos servidores da Google; ela recebeu um produto de inteligência pré-constituído por uma entidade privada, operando sob o que Pasquale (2015) define como *Black Box Society*: critérios algorítmicos opacos e protegidos por segredo industrial.

Trata-se, portanto, de uma Serendipidade Híbrida de Segundo Grau:

1. Primeiro grau (algorítmico): o algoritmo varre a nuvem e seleciona o que considera relevante para o contexto do CSAM, capturando, seja por contiguidade temporal ou por agrupamento de álbuns, os vídeos dos estupros hospitalares.

2. Segundo grau (humano): o agente estatal, ao auditar o pacote recebido para tipificar a pornografia infantil, descobre o crime de estupro de vulnerável adulto (Art. 217-A do Código Penal) (Rio de Janeiro, 2023).

A validação dessa prova revela o paradoxo do novo estatuto digital. Se não fosse o reporte automático legitimado pelo combate à adultização e exploração infantil, o Estado jamais teria acesso aos vídeos que condenaram o réu pelos crimes contra as pacientes adultas. A proteção da criança serviu, na prática, como um *bypass* jurídico que validou a devassa na nuvem do acusado, revelando delitos que, sob a ótica da privacidade tradicional, estariam blindados contra o escrutínio estatal.

A ausência de clareza sobre quais parâmetros levaram o algoritmo a incluir aqueles vídeos específicos no pacote reforça a necessidade de auditoria, visto que a "inteligência" privada acabou por ditar os rumos da persecução penal pública.

4.3 A materialização do risco: do "fruto da árvore envenenada" à validação judicial da custódia paralela

A entrada em vigor da Lei nº 15.211/2025 cristaliza um cenário de insegurança jurídica latente. Ao mesmo tempo em que o art. 27 obriga o reporte das plataformas, o art. 34, § 1º, veda a vigilância indiscriminada.

Essa antinomia normativa sugeria, teoricamente, que a defesa técnica poderia arguir a nulidade da prova algorítmica por excesso de escopo – a tese de que a IA, ao

analisar vídeos de adultos sem crianças, violou a privacidade de forma desproporcional, contaminando o processo pela Teoria dos Frutos da Árvore Envenenada.

Contudo, a análise dos desdobramentos processuais do Caso do anestesista (Ação Penal nº 0800337-68.2023.8.19.0058) demonstra que o Judiciário já começou a refutar essa tese, validando uma cadeia de custódia "paralela" e transnacional. Em sede de Embargos de Declaração, a defesa técnica sustentou expressamente a ocorrência de quebra da cadeia de custódia, alegando que os autos não continham os *reports* originais do NCMEC, mas apenas arquivos compilados em pen drive pela autoridade policial local (DCAV), o que comprometeria a rastreabilidade e a integridade da prova digital (Rio de Janeiro, 2023).

A resposta jurisdicional a esse incidente revela a atual *ratio decidendi* sobre o tema: a validação da prova não depende da custódia física tradicional, mas da convergência do fluxo de inteligência.

A sentença rejeitou a preliminar de nulidade, fundamentando que a defesa tentava aplicar à prova digital – descrita como "etérea e transnacional" – uma "lógica de custódia concebida para vestígios físicos", ignorando a realidade tecnológica e os protocolos de cooperação que sustentam a integridade dos dados.

Acolhendo a manifestação do Parquet, o decisum reconheceu a licitude do percurso da prova digital: da detecção pelo algoritmo do Google, passando pelo reporte ao NCMEC e à Polícia Federal, até o repasse à Polícia Civil. Ao invocar o princípio do *pas de nullité sans grief*, o magistrado considerou o conjunto probatório "robusto e convergente", superando a ausência dos arquivos originais do provedor nos autos do processo (Rio de Janeiro, 2023).

É imperioso ressaltar que a crítica à gênese da prova não implica defesa da conduta imputada ou busca pela impunidade, mas sim a preservação da higidez do sistema processual, pois a admissão de provas viciadas, a longo prazo, fragiliza a própria capacidade do Estado de punir agressores de forma definitiva.

Portanto, o que se observa na prática não é a anulação das investigações pelo risco do "fruto envenenado", mas a consolidação de uma jurisprudência que, em nome da proteção da infância, flexibiliza o rigor formal da cadeia de custódia (art. 158-A do CPP).

O sucesso da condenação neste leading case, longe de encerrar a discussão, serve de alerta: a dependência estatal da "polícia privada" algorítmica está sendo recepcionada pelos tribunais sob uma ótica de instrumentalidade das formas, exigindo, com ainda mais urgência, a adoção de filtros epistêmicos claros para que a validade da prova não dependa apenas da interpretação subjetiva sobre o "prejuízo", mas de standards auditáveis de legalidade.

4.4 O paradoxo da vigilância privada nos tribunais superiores: precedentes do STJ

Embora a doutrina aqui defendida aponte para a nulidade epistêmica dessas provas, é imperioso reconhecer que a praxis jurisprudencial atual do Superior Tribunal de Justiça caminha em sentido oposto, validando a cooperação baseada na confiança institucional (*good faith*) das *Big Techs*. Este artigo não ignora essa realidade; pelo contrário, utiliza-a como contraponto para demonstrar que a atual 'zona de conforto' do Judiciário está construída sobre alicerces frágeis que podem ruir diante de questionamentos técnicos mais sofisticados, como a Teoria do Mosaico.

A materialização do transbordamento de tutela observado no estudo de caso não é um evento isolado, mas reflete uma tensão dialética operante na jurisprudência recente dos tribunais superiores. A análise de acórdãos do Superior Tribunal de Justiça (STJ) confirma que a dependência estatal da *private search* cria um paradoxo: a eficiência na detecção algorítmica colide com a incapacidade estatal de processar a prova digital sem violar a integridade da cadeia de custódia.

O primeiro vetor desse paradoxo é a terceirização do início da persecução penal, validada nos conflitos de competência. No Conflito de Competência nº 212.717/SP (Brasil, 2025c), o STJ reconheceu que a investigação teve sua gênese no "Projeto Gênesis", acionado unicamente após o recebimento de informações reportadas por autoridades norte-americanas do NCMEC. A mesma dinâmica se repete no Conflito de Competência nº 210.185/AM (Brasil, 2025b), onde a competência jurisdicional foi definida pela natureza da detecção algorítmica transnacional.

Tais precedentes evidenciam que a Lei nº 15.211/2025 institucionaliza uma prática onde a soberania investigativa é parcialmente cedida à arquitetura de vigilância das *Big Techs*.

Contudo, essa eficiência na detecção esbarra no rigorismo epistêmico exigido para a condenação. O precedente firmado no Agravo Regimental no RHC nº 143.169/RJ (Caso Open Doors) atua como o "freio de arrumação" dessa lógica: o Ministro Ribeiro Dantas estabeleceu que a prova digital é volátil e que a ausência de garantias de integridade – como o uso de *hash* e espelhamento bit-a-bit – fulmina a validade da prova (Brasil, 2022).

Essa volatilidade é o ponto central da crítica de Quemel (2025), para quem a repercussão da quebra da cadeia de custódia deve ser modulada pela capacidade de auditoria da integridade do dado: sem documentação auditável, a prova é imprestável.

Mais recentemente, no Habeas Corpus nº 943.895/PR (Brasil, 2025d), o tribunal anulou provas derivadas de extração de dados móveis por falta de documentação auditável da cadeia de custódia. Essa jurisprudência demonstra que o transbordamento de tutela cria um sistema de "pesca probatória" eficiente na detecção, mas frágil na sustentação processual.

Sem um protocolo de recepção que traduza o input algorítmico privado em evidência forense pública auditável, a nova legislação corre o risco de inflar o sistema judiciário com inquéritos natimortos, anulados pela própria jurisprudência que busca proteger a integridade do processo penal.

5 POR UM PROTOCOLO DE SALVAGUARDA: DO "*BYPASS*" À CADEIA DE CUSTÓDIA PARALELA

Diante do cenário exposto – onde a vigilância algorítmica é inevitável por força da Lei nº 15.211/2025 e o "Transbordamento de Tutela" é uma realidade fática –, a solução não pode ser o ludismo jurídico (a rejeição total da tecnologia), nem o vale-tudo processual. A segurança jurídica da persecução penal exige o estabelecimento de standards probatórios que mitiguem o risco de nulidade.

5.1 A dialética da validade: credibilidade *versus* legalidade

O debate sobre a admissibilidade do relatório NCMEC/Big Tech no Brasil cinge-se, frequentemente, à integridade dos dados. De um lado, correntes garantistas apontam a quebra da cadeia de custódia (art. 158-A do CPP) na origem, visto que a coleta é feita por um ente privado sem supervisão estatal.

Prado (2024) aprofunda essa crítica ao desenvolver o conceito de "aspecto dinâmico da prova digital", argumentando que a volatilidade inerente ao dado exige dispositivos de controle epistêmico muito mais rigorosos do que os da prova física, sob pena de a cadeia de custódia tornar-se uma ficção burocrática incapaz de assegurar a mesmidade do elemento probatório.

Por outro lado, Fischer (2025) argumenta que a cadeia de custódia não é um fim em si mesmo, mas um instrumento para garantir a "fiabilidade" (*reliability*) da prova. Para esta corrente, eventuais falhas no trâmite não geram nulidade automática (iliceidade), mas apenas reduzem a credibilidade (peso) da prova, cabendo ao magistrado valorar essa redução na sentença. Pacelli e Fischer (2021) reforçam, em sua dogmática processual, que o sistema de nulidades deve ser orientado pelo princípio do prejuízo e pela instrumentalidade das formas, evitando que o formalismo excessivo impeça a apuração da verdade, desde que a essência da garantia não seja violada.

Entretanto, no contexto do "Transbordamento de Tutela", o problema é mais profundo que a mera fiabilidade. Quando a IA do Google vasculha a intimidade de um adulto buscando crimes infantis e encontra delitos diversos, o vício não é apenas de forma (cadeia de custódia), mas de fundamento constitucional (violação da privacidade e vedação à vigilância massiva do art. 34, § 1º, da nova lei) (Brasil, 2025a).

5.2 A proposta refinada: O Mandado de Verificação Preliminar (MVP) e a transmutação de inteligência em prova

Para superar o dilema entre a impunidade e a vigilância massiva, é imperativo abandonar a lógica binária ("tudo ou nada") na recepção da prova digital. A segurança

jurídica da persecução penal exige o estabelecimento de standards que convertam a eficiência tecnológica em robustez processual.

O relatório gerado pelo NCMEC ou pelas plataformas digitais não deve ser recepcionado automaticamente como prova plena, mas conceituado tecnicamente como Produto de Inteligência Cibernética. Conforme leciona Wendt (2024), a inteligência orienta a decisão, mas não se confunde com a evidência forense. Como tal, o *report* possui a função de nortear a investigação, mas carece de densidade epistêmica para autorizar, isoladamente e de plano, uma busca e apreensão genérica (general warrant) que devasse a totalidade da vida digital do suspeito.

Nesse sentido, propõe-se a instituição do Mandado de Verificação Preliminar (MVP) ou Busca Digital Fracionada. Este instrumento processual não visa burocratizar a investigação, mas sim conferir "imunidade processual" aos elementos colhidos, operando a transmutação do dado de inteligência (bruto) em evidência forense (auditável).

O protocolo opera através de três etapas de controle célere, inspiradas na lógica da *probable cause* progressiva extraída da *ratio decidendi* de *Carpenter v. United States* (Estados Unidos, 2018):

1. Etapa de congelamento (*Preservation Order*): ao receber o alerta algorítmico (inteligência), a autoridade policial solicita judicialmente a preservação imediata dos dados na *nuvem in dubio pro societate*. Esta medida cautelar visa garantir a "mesmidade" do dado e impedir que a prova seja destruída ou alterada. Trata-se de medida *inaudita altera pars*, de execução instantânea via ofício digital, que não atrasa a investigação, mas assegura a perenidade da cadeia de custódia conforme as preocupações de Prado (2024) quanto à volatilidade do suporte digital.

2. Etapa de validação específica (*The Peek-and-Confirm Doctrine*): superada a preservação, e diante da impossibilidade de corroboração por fontes abertas em crimes ocultos, o Estado realiza uma incursão cirúrgica. O juiz expede um mandado restrito autorizando a autoridade policial a acessar exclusivamente o arquivo hash reportado em ambiente controlado.

Não se trata de uma análise de mérito demorada, mas de uma Verificação de Tipicidade Técnica. Valendo-se da identidade única garantida pelo algoritmo de resumo

criptográfico, conforme detalha Jorge (2025), o agente estatal confirma se o arquivo reportado corresponde a um ilícito penal (visualização do CSAM) ou se trata de um falso positivo decorrente de colisão de *hash* ou descontextualização algorítmica (ex: fotos médicas ou artísticas), situações que demandam a confirmação humana para evitar erros judiciários automatizados.

É neste momento que ocorre a "lavagem" da prova: o input algorítmico privado é validado pelo crivo humano estatal, eliminando o risco de anulação por delegação de poder de polícia.

3. Etapa de busca plena (*Full Search Warrant*): somente após a confirmação estatal positiva na etapa anterior, expede-se o mandado de busca e apreensão amplo. Neste momento, a "justa causa" deixa de ser o algoritmo opaco de uma Big Tech e passa a ser a fé pública do agente policial que visualizou o ilícito na etapa 2.

Este novo mandado autoriza a apreensão de dispositivos e a varredura de outros arquivos, legitimada agora pela Teoria do Mosaico descrita por Kerr (2012). Estabelece-se, assim, um nexo de causalidade limpo: a busca plena não deriva do algoritmo do Google, mas da constatação policial visualizada na Etapa 2.

Essa proposta operacionaliza o que Matida e Vieira (2019) conceituam como a superação da dúvida razoável por etapas. O Estado reassume a soberania investigativa, garantindo que a "serendipidade híbrida" seja submetida ao devido processo legal.

Ressalte-se, por fim, que o MVP não atenta contra a celeridade ou a eficiência policial. Pelo contrário, atua como salvaguarda da própria operação. Ao exigir essa validação prévia – que pode ser realizada em questão de horas em regime de plantão judiciário –, o sistema blinda a investigação contra teses de nulidade baseadas na "doutrina da busca privada" ou no "fruto da árvore envenenada".

Evita-se, assim, que a IA atue como um "juiz de instrução" automatizado e garante-se que a condenação do agressor seja sustentável nos tribunais superiores, impedindo que criminosos reais se beneficiem de falhas procedimentais estatais.

6 CONSIDERAÇÕES FINAIS

A trajetória percorrida neste estudo confirma a hipótese inicial de que a Lei nº 15.211/2025, ao automatizar a vigilância digital sob o pretexto de combater a adultização, instituiu um fenômeno de "Transbordamento de Tutela". Restou demonstrado que a delegação irrestrita da atividade investigativa aos algoritmos privados rompe a cadeia de custódia e subverte a lógica constitucional, transformando a exceção da busca privada em regra de monitoramento massivo.

A "serendipidade híbrida", portanto, quando desprovida de controle, não gera prova, mas sim um elemento informativo viciado pela opacidade da "caixa-preta" das plataformas.

Contudo, a proteção integral da infância e juventude no ciberespaço não admite retrocessos luditas. A ineficácia dos métodos analógicos diante do volume de crimes cibernéticos impõe o uso de Inteligência Artificial. O nó górdio desatado por esta pesquisa não reside na tecnologia em si, mas na presunção de veracidade absoluta conferida aos seus resultados.

A segurança jurídica exige que o Estado abandone a postura de mero homologador de relatórios corporativos.

Diante disso, a admissibilidade da prova digital oriunda desse monitoramento deve ser condicionada à implementação do Protocolo de Verificação Preliminar. Este mecanismo, proposto como filtro de contenção, exige que a defesa e o magistrado tenham acesso não apenas ao "flagrante" final, mas aos metadados de origem e ao código *hash* da captura inicial, permitindo a auditabilidade do caminho percorrido pelo algoritmo.

Somente através deste protocolo é possível transmutar a "inteligência privada" (dado bruto) em "evidência forense" (prova válida).

Em suma, o combate à adultização e a garantia da cibersegurança não são vetores excludentes, desde que o processo penal recupere sua soberania epistêmica. Ao adotar o Protocolo de Verificação Preliminar, o sistema de justiça assegura que a luta contra a adultização precoce e a exploração infantil não sirva de salvo-conduto para a erosão da privacidade do cidadão, restabelecendo o equilíbrio necessário para que a cibersegurança

cumpra seu papel de blindagem do desenvolvimento infantojuvenil sem, contudo, tutelar autoritariamente a liberdade do adulto.

Afinal, uma sociedade que infantiliza seus adultos perde a capacidade de proteger verdadeiramente suas crianças.

REFERÊNCIAS

ABREU, Jacqueline de Souza. Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience. **Revista de Informação Legislativa**, Brasília, DF, v. 55, n. 218, p. 77-102, abr./jun. 2018. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/552776/001139852.pdf. Acesso em: 14 dez. 2025.

BRASIL. [Lei nº 15.211 (2025)]. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais. **Diário Oficial da União**, Brasília, DF, 17 set. 2025a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 14 dez. 2025.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ. Relator: Min. Ribeiro Dantas. **Diário da Justiça Eletrônico**, Brasília, DF, 25 out. 2022.

BRASIL. Superior Tribunal de Justiça. Conflito de Competência nº 210.185/AM. Relator: Min. Sebastião Reis Júnior. **Diário da Justiça Eletrônico**, Brasília, DF, 21 jan. 2025b.

BRASIL. Superior Tribunal de Justiça. Conflito de Competência nº 212.717/SP. Relator: Min. Reynaldo Soares da Fonseca. **Diário da Justiça Eletrônico**, Brasília, DF, 24 abr. 2025c.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 943.895/PR. Relator: Min. Joel Ilan Paciornik. **Diário da Justiça Eletrônico**, Brasília, DF, 21 fev. 2025d.

DIAS, Bruna Mariano Coutinho. A cooperação jurídica internacional e a produção da prova digital: uma análise das ferramentas previstas na Convenção de Budapeste. **Portal de Trabalhos Acadêmicos**, [S. l.], v. 18, n. 1, 2025. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/academico/article/view/3230. Acesso em: 15 dez. 2025.

ESTADOS UNIDOS. [U.S. Code (2024)]. Title 18: Crimes and Criminal Procedure. Section 2258A: Reporting requirements of providers. Washington, DC: Office of the

Law Revision Counsel, 2024. Disponível em: https://uscode.house.gov. Acesso em: 14 dez. 2025.

ESTADOS UNIDOS. Supreme Court. **Carpenter v. United States**, 138 S. Ct. 2206 (2018). Washington, DC: Supreme Court of the United States, 2018.

ESTADOS UNIDOS. Supreme Court. **United States v. Jacobsen**. 466 U.S. 109. Washington, DC, 2 abr. 1984. Disponível em: https://supreme.justia.com/cases/federal/us/466/109/. Acesso em: 15 dez. 2025.

ESTADOS UNIDOS. Supreme Court. **United States v. Jones**. 565 U.S. 400. Washington, DC, 23 jan. 2012. Disponível em: https://supreme.justia.com/cases/federal/us/565/400/. Acesso em: 15 dez. 2025.

FISCHER, Douglas. A cadeia de custódia envolve a aferição da mesmidade ou fiabilidade da prova, não a sua invalidade/nulidade. **Temas Jurídicos**, [S. l.], 11 set. 2025. Disponível em: https://temasjuridicospdf.com/. Acesso em: 15 dez. 2025.

GOOGLE. **Termos de Serviço do Google**. Mountain View: Google, 2025. Disponível em: https://policies.google.com/terms. Acesso em: 14 dez. 2025.

JORGE, Higor Vinicius Nogueira. **Manual de Investigação Criminal Tecnológica**. 4. ed. Salvador: JusPodivm, 2025.

KERR, Orin S. The Mosaic Theory of the Fourth Amendment. **Michigan Law Review**, Ann Arbor, v. 111, n. 3, p. 311-354, 2012.

LIMA, Eduardo Pacheco de Mello; LIMA, Anderson Rodrigo Andrade de. Report do NCMEC: da admissibilidade como prova pelo ordenamento jurídico brasileiro. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 7., 2024, Santa Maria. **Anais [...]**. Santa Maria: UFSM, 2024. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2024/12/2.3.pdf. Acesso em: 15 dez. 2025.

MATIDA, Janaina; VIEIRA, Antonio. Para além do BARD: uma crítica à crescente adoção do standard de prova "beyond a reasonable doubt" no processo penal brasileiro. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 27, n. 156, p. 221-248, jun. 2019. Disponível em: https://bd.tjdft.jus.br/items/12627bf6-a38e-4a84-bc91-0b5845b32a1e. Acesso em: 15 dez. 2025.

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN. **CyberTipline Data 2023**. Alexandria, VA: NCMEC, 2024. Disponível em: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata. Acesso em: 15 dez. 2025.

PACELLI, Eugênio; FISCHER, Douglas. **Comentários ao Código de Processo Penal e sua Jurisprudência**. 13. ed. rev., atual. e ampl. São Paulo: Atlas, 2021.

PASQUALE, Frank. **The Black Box Society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PRADO, Geraldo. Esboço de proposta sobre dispositivo de controle da investigação digital: O "aspecto dinâmico da prova digital". **Revista do Sistema Único de Segurança Pública**, Brasília, v. 3, n. 1, p. 240–261, 2024. DOI: 10.56081/revsusp.v3i1.621. Disponível em: https://revistasusp.mj.gov.br/susp/index.php/revistasusp/article/view/621. Acesso em: 15 dez. 2025.

QUEMEL, Melhym Pereira. A integridade da prova digital como vetor da modulação da nulidade: repercussões da quebra da cadeia de custódia. **Revista do CNMP**, Brasília, v. 13, p. 236-259, 2025. Disponível em: https://ojs.cnmp.mp.br/index.php/revistacnmp/article/view/845/614. Acesso em: 14 dez. 2025.

RIO DE JANEIRO. Tribunal de Justiça. **Ação Penal nº 0800337-68.2023.8.19.0058**. Réu: A. E. O. C. Rio de Janeiro: TJRJ, 2023.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico**. 6. ed. São Paulo: SaraivaJur, 2022.

TEUBNER, Gunther. **Fragmentos constitucionais**: constitucionalismo social na globalização. São Paulo: Saraiva, 2016.

WENDT, Emerson. **Investigação Criminal Cibernética no Brasil**. Leme: Mizuno, 2024.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.