Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i11.32611

A REGULAMENTAÇÃO DAS REDES SOCIAIS NO BRASIL E OS DESAFIOS DA PERSECUÇÃO PENAL DE CRIMES CONTRA CRIANÇAS E ADOLESCENTES NO AMBIENTE DIGITAL

THE REGULATION OF SOCIAL MEDIA IN BRAZIL AND THE CHALLENGES OF CRIMINAL PROSECUTION FOR CRIMES AGAINST CHILDREN AND ADOLESCENTS IN THE DIGITAL ENVIRONMENT

LA REGULACIÓN DE LAS REDES SOCIALES EN BRASIL Y LOS DESAFÍOS DE LA PERSECUCIÓN PENAL DE DELITOS CONTRA NIÑOS Y ADOLESCENTES EN EL ENTORNO DIGITAL

Luis Felipe Gomes de Sousa[1]
Juliano de Oliveira Leonel[2]

RESUMO: A expansão das redes sociais e o uso crescente de tecnologias digitais por crianças e adolescentes reconfiguraram as dinâmicas de sociabilidade no ciberespaço, ampliando a exposição do público infantojuvenil a condutas ilícitas que desafiam os mecanismos tradicionais do Direito. Para tanto, esta discussão tem como objetivo geral analisar em que medida o modelo jurídico brasileiro de regulamentação das redes sociais e de persecução penal se mostra adequado à proteção de crianças e adolescentes contra crimes praticados no ambiente digital. Metodologicamente, o trabalho é guiado por uma abordagem qualitativa e de natureza não experimental, com caráter exploratório e descritivo, recorrendo à pesquisa bibliográfica e documental a partir do exame do Marco Civil da Internet, da Lei nº 14.811/2024 e do ECA Digital (Lei nº 15.211/2025), utilizando principais autores tais como Aury Lopes Jr., Gustavo Badaró, Ana Frazão, Marta Saad Gimenes, Pierre Lévy e Manuel Castells. Ao final, o estudo alcança como resultado a constatação de que o modelo jurídico brasileiro evoluiu com o dever geral de cuidado das plataformas e novos instrumentos de investigação, mas sua efetividade prática permanece limitada por entraves na preservação da cadeia de custódia e na cooperação com big techs.

Palavras-chave: Regulamentação de Redes Sociais. ECA Digital. Persecução Penal. Prova Digital. Cadeia de Custódia.

ABSTRACT: The expansion of social media and the increasing use of digital technologies by children and adolescents have reconfigured social dynamics in cyberspace, increasing the exposure of minors to illicit conduct that challenges traditional legal mechanisms. Therefore, this discussion aims to analyze to what extent the Brazilian legal framework for social media regulation and criminal prosecution is adequate for protecting children and adolescents against cybercrimes. Methodologically, the study adopts a qualitative, non-experimental, exploratory, and descriptive approach, utilizing bibliographic and documentary research based on the Civil Framework for the Internet, Law No. 14,811/2024, and the Digital ECA (Law No. 15,211/2025), relying on key authors such as Aury Lopes Jr., Gustavo Badaró, Ana Frazão, Marta Saad Gimenes, Pierre Lévy, and Manuel Castells. Ultimately, the study concludes that while the Brazilian legal framework has evolved through the establishment of a duty of care for platforms and new investigative tools, its practical effectiveness remains limited by challenges in preserving the chain of custody and securing cooperation with big tech companies.

[1] Graduando em Direito. Centro Universitário Santo Agostinho (UNIFSA).
[2] Doutor em Ciências Criminais pela PUCRS. Mestre em Direito pela UCB. Professor. Orientador. Centro Universitário Santo Agostinho (UNIFSA).

Keywords: Social Media Regulation. Digital ECA. Criminal Prosecution. Digital Evidence. Chain of Custody.

RESUMEN: La expansión de las redes sociales y el uso creciente de tecnologías digitales por niños y adolescentes han reconfigurado las dinámicas de sociabilidad en el ciberespacio, ampliando la exposición del público infantojuvenil a conductas ilícitas que desafían los mecanismos tradicionales del Derecho. Para ello, esta discusión tiene como objetivo general analizar en qué medida el modelo jurídico brasileño de regulación de redes sociales y persecución penal resulta adecuado para la protección de menores frente a delitos digitales. Metodológicamente, el estudio adopta un enfoque cualitativo y no experimental, exploratorio y descriptivo, recurriendo a la investigación bibliográfica y documental basada en el Marco Civil de Internet, la Ley nº 14.811/2024 y el ECA Digital (Ley nº 15.211/2025), sustentada en autores como Aury Lopes Jr., Gustavo Badaró, Ana Frazão, Marta Saad Gimenes, Pierre Lévy y Manuel Castells. Al final, se concluye que el modelo jurídico ha evolucionado con el deber general de cuidado de las plataformas y nuevos instrumentos de investigación, pero su efectividad práctica sigue limitada por obstáculos en la cadena de custodia y en la cooperación con las grandes tecnológicas.

Palabras clave: Regulación de Redes Sociales. ECA Digital. Persecución Penal. Prueba Digital. Cadena de Custodia.

1 INTRODUÇÃO

A expansão das redes sociais como espaço central de interação social tem produzido impactos relevantes na tutela jurídica de direitos fundamentais, especialmente no que se refere à proteção de crianças e adolescentes no ambiente digital. A intensificação do uso dessas plataformas, aliada à velocidade de circulação de informações e à amplitude de alcance das interações virtuais, favorece o surgimento de condutas ilícitas que desafiam os mecanismos tradicionais de controle e repressão do Direito Penal e do Processo Penal.

A investigação foi construída a partir da seguinte problematização: em que medida o modelo jurídico brasileiro de regulamentação das redes sociais e de persecução penal se mostra adequado à proteção de crianças e adolescentes contra crimes praticados no ambiente digital? A partir desse problema, formulou-se o objetivo geral de analisar em que medida o modelo jurídico brasileiro de regulamentação das redes sociais e de persecução penal atende às exigências de proteção do público infantojuvenil frente às especificidades dos crimes virtuais.

A justificativa da pesquisa fundamenta-se na sua relevância social, científica e pessoal. Sob o prisma social, justifica-se diante da necessidade prática de avaliar se o ordenamento jurídico dispõe de instrumentos eficazes para salvaguardar crianças e adolescentes de práticas que atentam contra sua dignidade. No plano científico e acadêmico, o estudo contribui para o debate sobre a adaptação do sistema de justiça criminal às novas formas de criminalidade decorrentes das transformações tecnológicas, preenchendo lacunas sobre a relação entre regulação de redes e persecução penal. No âmbito pessoal, decorre do interesse em aprofundar a pesquisa na intersecção entre Direito Digital, Direito Penal e Direito Processual Penal.

Metodologicamente, o estudo classifica-se quanto à natureza como pesquisa básica e quanto à abordagem como qualitativa, de caráter não experimental, exploratório e descritivo, aplicando o método jurídico-dogmático e hermenêutico. A coleta de dados realizou-se por meio de levantamento bibliográfico e documental, examinando o Marco Civil da Internet (Lei nº 12.965/2014), a Lei nº 14.811/2024, o ECA Digital (Lei nº 15.211/2025) e a legislação correlata. A fundamentação amparou-se em autores referenciais como Aury Lopes Jr., Gustavo Badaró, Marta Saad Gimenes, Ana Frazão, Elora Fernandes, Pierre Lévy, Manuel Castells e José van Dijck.

Para tanto, este estudo está dividido em três seções de desenvolvimento. A primeira seção, intitulada "A tutela protetiva da infância no ambiente digital e o marco regulatório das redes sociais no Brasil", tem como objetivo investigar a evolução dos crimes digitais, a proteção integral e a regulamentação das redes sociais à luz do Marco Civil da Internet, da Lei nº 14.811/2024 e do ECA Digital.

A segunda seção, direcionada como "Os desafios da persecução penal e a disciplina da prova digital", visa verificar os principais desafios da investigação criminal, com foco na identificação de autores, na produção e preservação da prova digital e na atuação institucional do Ministério Público e das Polícias Judiciárias.

A terceira seção, denominada "Os limites da jurisdição e a cooperação com provedores de aplicação", tem por objetivo analisar a incidência da jurisdição nacional, os regimes de requisição de dados e os mecanismos formais e multilaterais de cooperação jurídica internacional.

2 A TUTELA PROTETIVA DA INFÂNCIA NO AMBIENTE DIGITAL E O MARCO REGULATÓRIO DAS REDES SOCIAIS NO BRASIL

Esta sessão introduz o presente artigo examinando a proteção de crianças e adolescentes no ecossistema digital a partir do princípio da proteção integral (art. 227 da CF/88). Para isso, analisa-se a evolução das tecnologias, as dinâmicas sociais, bem como a transformação das comunicações e o marco regulatório brasileiro, desde as premissas do Marco Civil da Internet até a consolidação do ECA Digital (Lei nº 15.211/2025), que estabelece o dever geral de cuidado das plataformas. Por fim, delineiam-se os aspectos dogmáticos dos crimes cibernéticos contra a dignidade sexual infantojuvenil no Código Penal e no Estatuto da Criança e do Adolescente.

2.1 Sociedade da informação, platform society e a proteção integral no ciberespaço

O desenvolvimento das tecnologias de informação reconfigurou as estruturas sociais e as dinâmicas de sociabilidade. Lévy (2010) conceitua o ciberespaço como um ambiente de comunicação e interação constituído pela interconexão mundial de computadores, cuja expansão produz novas formas de relacionamento e circulação do conhecimento.

Na mesma linha, Castells (2005) caracteriza a sociedade em rede como uma estrutura marcada pela centralidade das tecnologias digitais na organização das relações sociais, econômicas e culturais. Mais recentemente, van Dijck, Poell e De Waal (2018) introduziram o conceito de platform society para descrever como plataformas digitais assumiram a mediação central das interações cotidianas e da circulação de dados na esfera pública.

A inserção de crianças e adolescentes nesse ecossistema amplifica as oportunidades de aprendizado e exercício de direitos, mas os expõe a riscos severos de exposição, discriminação e exploração sexual. Conforme apontam Reis e Jacob (2025), a massificação do acesso precoce de infantes à rede, frequentemente despida de mediação familiar ou de filtros de segurança, acentua a coleta indiscriminada de dados pessoais.

Amparados nas premissas de proteção de dados, Reis e Jacob (2025) destacam que a proteção da privacidade de menores na internet deixou de ser uma salvaguarda individual meramente patrimonial para se converter em pressuposto fundamental da garantia de sua integridade física, psíquica e moral no ciberespaço.

Diante dessa vulnerabilidade, o ordenamento jurídico brasileiro adota a Doutrina da Proteção Integral, consagrada no art. 227 da Constituição Federal de 1988 e estruturada pelo Estatuto da Criança e do Adolescente (Lei nº 8.069/1990). O preceito constitucional estabelece o dever tríplice e solidário da família, da sociedade e do Estado de assegurar ao público infantojuvenil, com absoluta prioridade, o direito à vida, à dignidade e à proteção contra toda forma de violência e opressão:

> É dever da família, da comunidade, da sociedade em geral e do Poder Público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária.

No plano internacional, o Comitê dos Direitos da Criança das Nações Unidas, no Comentário Geral nº 25 (2021), assentou expressamente (UNITED NATIONS, 2021) que os direitos humanos reconhecidos na Convenção sobre os Direitos da Criança aplicam-se com igual rigor ao ambiente digital. Assegura-se, assim, que a proteção no ambiente virtual não deve

ser compreendida apenas como restrição de acesso, mas como a garantia de privacidade, segurança por padrão e desenvolvimento progressivo da autonomia.

Conforme destacam Peixoto, Bueno e Pereira (2024), a complexidade das interações em rede exige redistribuir os deveres de cuidado, de modo que a responsabilidade não recaia exclusivamente sobre o núcleo familiar, alcançando também os agentes econômicos operadores de serviços tecnológicos.

2.2 Da disciplina do Marco Civil da Internet ao dever geral de cuidado do ECA Digital

O arcabouço normativo das redes no Brasil teve como marco fundamental a Lei nº 12.965/2014 (Marco Civil da Internet), que estabeleceu princípios, garantias, direitos e deveres para o uso da rede, resguardando a liberdade de expressão, a privacidade e a proteção de dados (SOUZA; LEMOS, 2016).

Contudo, a regra geral insculpida no art. 19 do Marco Civil — que condicionava a responsabilidade civil do provedor por danos decorrentes de conteúdo de terceiros à prévia e específica ordem judicial — revelou-se insuficiente para conter a proliferação de ilícitos sistêmicos praticados contra vulneráveis. Essa limitação motivou a recente releitura do dispositivo pelo Supremo Tribunal Federal no Tema 533 da Repercussão Geral (SUPREMO TRIBUNAL FEDERAL, 2026).

A insuficiência do modelo tradicional de notificação judicial posterior ensejou a promulgação da Lei nº 15.211/2025 (ECA Digital), inaugurando uma abordagem focada na prevenção e na mitigação de riscos. O novo diploma impõe obrigações aos fornecedores de produtos e serviços de tecnologia acessíveis a crianças e adolescentes, estabelecendo a aplicação de diretrizes de proteção desde a concepção dos serviços (safety by design).

Como leciona Fernandes (2021), a arquitetura dos sistemas digitais deve ser projetada para resguardar a privacidade e a segurança do usuário hipervulnerável, impedindo que a proteção dependa tão somente de remoções reativas do conteúdo danoso.

Dentre as obrigações instituídas pela Lei nº 15.211/2025, destacam-se a verificação etária adequada, a vinculação de contas de menores de 16 anos aos seus responsáveis legais (art. 24), a proibição de criação de perfis comportamentais para direcionamento de publicidade comercial (art. 26) e o dever de remoção imediata e notificação às autoridades nos casos de suspeita de exploração sexual, abuso, sequestro ou aliciamento (art. 27).

A instituição desse regime dialoga com a doutrina de Frazão (2023) e Reis e Jacob (2025), que sustentam a existência de um dever geral de cuidado aplicável às big techs, exigindo postura proativa, responsável e transparente diante dos impactos sociais de seus algoritmos.

2.3 Tipicidade penal e a dogmática dos crimes virtuais contra crianças e adolescentes

A transposição das condutas ilícitas para os meios virtuais exige rigoroso enquadramento dogmático no Direito Penal. Sob a perspectiva dogmática do Direito Penal, cumpre diferenciar os crimes informáticos puros ou próprios (aqueles em que o sistema informático ou os dados em si figuram como objeto material e bem jurídico tutelado) dos crimes informáticos mistos ou impróprios (nos quais a internet atua como mero meio de execução para atingir bens jurídicos preexistentes, como a honra e a dignidade sexual).

Como ponderam Barbosa (2024) e Araújo (2024), delitos gravíssimos como o estupro de vulnerável (art. 217-A do Código Penal) mantêm seus elementos objetivos e subjetivos inalterados quando praticados via meio digital. Da mesma forma, a categoria médica "pedofilia" não equivale a um tipo penal autônomo, exigindo-se a perfeita adequação da conduta aos ilícitos previstos no Código Penal ou no ECA.

No âmbito das condutas adaptadas ao meio virtual, destaca-se o fenômeno do grooming (aliciamento digital), em que agressores usufruem do disfarce das telas e da comunicação instantânea para seduzir e manipular vítimas vulneráveis. Paralelamente, Araújo (2024) evidencia que o assédio moral sistemático no ambiente virtual — o cyberbullying — atinge níveis de lesividade e angústia contínua superiores aos de suas modalidades analógicas, dada a ausência de fronteiras físicas ou temporais.

Além disso, Barbosa (2024) pontua que a emergência da Inteligência Artificial e a produção de conteúdos sintéticos (deepfakes e deepnudes) alteraram a fronteira das agressões sexuais, permitindo violações gravíssimas aos direitos da personalidade e à integridade psíquica da criança sem a necessidade de captura de sua imagem física real.

O Estatuto da Criança e do Adolescente contempla tipificações penais específicas destinadas a coibir a violência sexual digital nos arts. 240 e seguintes. Esses dispositivos punem severamente as condutas de produzir, reproduzir, transmitir, divulgar, disponibilizar, adquirir, possuir e armazenar conteúdos de pornografia e violência sexual envolvendo crianças ou adolescentes.

O arcabouço penal foi aperfeiçoado pela Lei nº 14.811/2024 — que tipificou o bullying e o cyberbullying no Código Penal e alçou condutas do ECA ao rol de crimes hediondos (Lei nº

8.072/1990) (ARAUJO, 2024) — e pela Lei nº 15.487/2026, alcançando ilícitos praticados em jogos on-line, fóruns, redes sociais e mediante ferramentas de Inteligência Artificial (BRASIL, 1990; BRASIL, 2024, 2026).

Em que pese a evolução da dogmática e o endurecimento das redações penais, a efetividade da tutela estatal desloca-se para o plano da investigação e da persecução penal. A volatilidade das evidências eletrônicas e a sofisticação das técnicas de ocultação de identidade colocam em xeque a resposta jurisdicional, exigindo o exame dos instrumentos de colheita probatória e das garantias processuais aplicáveis à prova digital.

3 OS DESAFIOS DA PERSECUÇÃO PENAL E A DISCIPLINA DA PROVA DIGITAL

Esta sessão aborda os principais obstáculos operacionais e procedimentais enfrentados pela investigação criminal no ambiente cibernético. Examina-se a implementação de novos instrumentos investigativos, como a ronda virtual e a infiltração de agentes virtuais, bem como a relevância da porta lógica de origem para a identificação de autoria em redes compartilhadas. Além disso, analisa-se a disciplina da prova digital e as exigências da cadeia de custódia (arts. 158-A a 158-F do CPP) sob a ótica da jurisprudência dos tribunais superiores e das atribuições das Polícias Judiciárias e do Ministério Público.

3.1 A persecução penal no ambiente digital e os novos instrumentos investigativos

A apuração de infrações penais praticadas por meio de redes sociais e aplicações de internet submete-se às garantias constitucionais do devido processo legal, sem prejuízo da observância de especificidades inerentes à volatilidade do meio digital. A persecução penal abrange as fases pré-processual e processual, visando à colheita de elementos de informação sobre a materialidade e a autoria delitiva.

Como lecionam Saad Gimenes, Rossi e Partata (2024), a colheita da prova digital atinge diretamente direitos fundamentais como a intimidade, o sigilo das comunicações e a autodeterminação informativa, o que exige estrito cumprimento dos requisitos legais sob pena de ilicitude probatória.

Diante do aumento da gravidade e da complexidade das condutas praticadas contra o público infantojuvenil no ambiente cibernético, a Lei nº 15.487/2026 introduziu modificações expressas no Estatuto da Criança e do Adolescente para modernizar as técnicas de investigação, destacando-se o art. 190-F do ECA, que disciplinou a chamada "ronda virtual" (BRASIL, 1990;

BRASIL, 2026). Trata-se do monitoramento e da coleta automatizada de arquivos e conteúdos de violência sexual disponibilizados em ambientes virtuais públicos.

Em contrapartida, o ordenamento jurídico já contemplava a infiltração virtual de agentes policiais. Todavia, Araújo (2024) salienta que a efetividade dessa técnica avançada enfrenta sérias barreiras estruturais, tais como a escassez de recursos tecnológicos nas delegacias especializadas, a falta de capacitação técnica continuada e a morosidade cartorária.

A instituição de técnicas proativas reflete a busca por respostas estatais celeres diante da disseminação de conteúdos ilícitos em fóruns, redes sociais e redes P2P (peer-to-peer). Contudo, tais medidas não equivalem a autorização irrestrita para a devassa da esfera privada.

O art. 190-F, §§ 2º e 3º, do ECA limita a requisição direta de dados cadastrais ou registros de conexão sem prévia ordem judicial às hipóteses de flagrante delito ou de risco iminente à vida ou à integridade física da criança ou adolescente, impondo comunicação posterior ao Judiciário em 48 horas (BRASIL, 1990; BRASIL, 2026). Preserva-se, desse modo, a reserva de jurisdição e o sigilo de dados.

3.2 Identificação de autoria: registros de conexão, de aplicação e a relevância da porta lógica de origem

A vinculação de uma conduta ilícita praticada no ambiente virtual a um indivíduo determinado constitui um dos gargalos mais complexos da investigação criminal cibernética. O Marco Civil da Internet (Lei nº 12.965/2014) fixou premissas técnicas essenciais ao diferenciar os registros de conexão dos registros de acesso a aplicações de internet. Enquanto os registros de conexão abrangem a data, a hora de início e término, a duração e o endereço IP utilizado pelo terminal, os registros de aplicação correspondem ao conjunto de informações relativas à data e à hora de uso de uma aplicação específica a partir de determinado endereço IP (BRASIL, 2014).

A identificação precisa do terminal tornou-se ainda mais complexa com o esgotamento dos endereços no protocolo IPv4 e a consequente adoção de técnicas de compartilhamento de IPs por múltiplos usuários via CGNAT (Carrier-Grade NAT). Nesses cenários, a simples indicação do endereço IP é insuficiente para individualizar a conexão, tornando indispensável a identificação da porta lógica de origem.

No plano jurisprudencial, o Superior Tribunal de Justiça consolidou entendimento no REsp 2.170.872/SP de que a identificação da porta lógica deve pautar-se pela utilidade e pela possibilidade concreta de individualização do usuário (SUPERIOR TRIBUNAL DE JUSTIÇA, 2025b). Todavia, os dados técnicos obtidos junto aos provedores indicam o terminal

ou conexão, mas não se confundem automaticamente com a autoria delitiva. A atribuição de responsabilidade penal requer a convergência probatória entre os registros de rede, a perícia em dispositivos apreendidos e os demais elementos do inquérito policial.

Ademais, é técnica e pragmaticamente imprescindível distinguir a preservação cautelar dos dados do seu efetivo fornecimento às autoridades. Os arts. 13, § 2º, e 15, § 2º, do Marco Civil da Internet autorizam a requisição administrativa de preservação de registros por prazo superior ao legal (BRASIL, 2014). No AgRg no HC 998.395/SP, o STJ reafirmou a validade da preservação administrativa cautelar emergencial, ressaltando que o fornecimento e acesso ao conteúdo dos registros permanecem condicionados à prévia autorização judicial (SUPERIOR TRIBUNAL DE JUSTIÇA, 2025a).

3.3 A prova digital e os parâmetros da cadeia de custódia

A centralidade da prova digital no processo penal contemporâneo impõe o rigoroso cumprimento das regras de integridade, autenticidade e auditabilidade dos vestígios eletrônicos. Inseridos no Código de Processo Penal pela Lei nº 13.964/2019 (Pacote Anticrime), os arts. 158-A a 158-F conceituam a cadeia de custódia como o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio (BRASIL, 1941; BRASIL, 2019).

Conforme leciona Júnior (2026), dispositivos eletrônicos como smartphones e tablets constituem arcabouços robustos de dados pessoais, metadados, PINs e geolocalização, mas a prova digital em formato binário (0 e 1) exige procedimentos técnicos complexos de extração e documentação. A manipulação indevida ou a ausência de métodos científicos de extração forense podem causar a nulidade insanável da prova em juízo.

Badaró (2021) enfatiza a necessidade de observância dos standards metodológicos (espelhamento e hash), enquanto Badaró Massena (2023) aponta que a quebra da cadeia de custódia acentua a assimetria informacional entre acusação e defesa, violando o contraditório e a ampla defesa. Nessa perspectiva, Reis e Jacob (2025), amparados na doutrina de Aury Lopes Jr., reiteram que a urgência na repressão aos crimes digitais contra vulneráveis não autoriza relativizar as garantias constitucionais do devido processo legal.

Analisando os impactos processuais das irregularidades na colheita da prova digital, o STJ fixou orientação no AgRg no HC 1.014.212/ES, decidindo que, havendo dúvida razoável quanto à integridade ou autenticidade dos dados digitais que fundamentam a acusação, torna-se indispensável a realização de perícia técnica para atestar sua fidedignidade (SUPERIOR TRIBUNAL DE JUSTIÇA, 2026a).

Por outro lado, na linha do entendimento firmado no Inq 1.674/DF, a Corte Especial do STJ ponderou que o uso da função hash constitui mecanismo eficaz de validação, mas sua ausência pontual em fases de coleta preliminar não acarreta a nulidade automática se a autenticidade puder ser demonstrada por outros meios hígidos (SUPERIOR TRIBUNAL DE JUSTIÇA, 2026b).

3.4 Atribuições institucionais do Ministério Público e das polícias judiciárias

A consecução da persecução penal cibernética fundamenta-se na repartição constitucional de competências entre as Polícias Judiciárias (Civil e Federal) e o Ministério Público. Às Polícias Judiciárias incumbe a condução do inquérito policial e a execução de diligências e perícias, ao passo que ao Ministério Público cabe o controle externo da atividade policial e a titularidade privativa da ação penal pública (art. 129, I e VIII, da CF/88).

No julgamento do Tema 184 da Repercussão Geral (RE 593.727/MG), o Supremo Tribunal Federal fixou a tese de que o Ministério Público dispõe de competência própria para promover investigações de natureza penal, desde que respeitadas as garantias fundamentais, as hipóteses de reserva de jurisdição e o controle judicial (SUPREMO TRIBUNAL FEDERAL, 2015). Essa prerrogativa investigativa direta assume relevância no enfrentamento da criminalidade digital contra vulneráveis, especialmente com a atuação incisiva fixada pelo ECA Digital (Lei nº 15.211/2025) na fiscalização de redes sociais, jogos e serviços de streaming.

Entretanto, a cooperação e a atuação investigativa das instituições não eliminam as balizas legais impostas à colheita da prova. A condução de rondas virtuais e a requisição direta de dados cadastrais devem observar rigorosamente as hipóteses do art. 190-F do ECA, sob pena de usurpação de competência judicial e ilicitude probatória (BRASIL, 1990; BRASIL, 2026). A eficiência do combate aos crimes virtuais exige, portanto, atuação sinérgica, técnica e articulada das instituições da persecução penal, resguardando sempre os limites constitucionais e o devido processo legal.

4 OS LIMITES DA JURISDIÇÃO E A COOPERAÇÃO COM PROVEDORES DE APLICAÇÃO

Esta sessão analisa a atuação das plataformas digitais e os limites territoriais da jurisdição brasileira frente à natureza transnacional da internet. Discutem-se os deveres de colaboração das big techs e os regimes jurídicos para requisição de dados cadastrais, registros e conteúdos de comunicação. Em seguida, examina-se a aplicação da regra de territorialidade

prevista no art. 11 do Marco Civil da Internet à luz da ADC 51/DF do Supremo Tribunal Federal, assim como o papel da Convenção de Budapeste na cooperação jurídica internacional para a obtenção expedita de provas mantidas no exterior.

4.1 A atuação das plataformas digitais e os deveres de colaboração na persecução penal

A posição central que as plataformas digitais ocupam no ecossistema das comunicações exige a clara delimitação do seu papel no combate a ilícitos cibernéticos. Embora os seus serviços sejam rotineiramente utilizados como meio de execução ou armazenamento de provas de crimes contra a infância, as big techs não ostentam natureza de órgãos de segurança pública ou de investigação privada.

Como leciona Frazão (2023), a atuação desses agentes privados é delimitada por deveres legais específicos de cuidado, prevenção de riscos e colaboração com o Estado, em estrita consonância com a prioridade absoluta constitucionalmente assegurada às crianças e aos adolescentes.

Nesse cenário, conforme ponderam Reis e Jacob (2025) e Araújo (2024), as plataformas possuem ferramentas técnicas para atuar de forma proativa, tais como o banimento e restrição de usuários suspeitos por meio da monitoração de histórico de pesquisas, filtros de hashtags, sistemas de verificação facial e aferição etária instituídos pelo ECA Digital (Lei nº 15.211/2025). Contudo, tais medidas de moderação proativa devem ser implementadas em harmonia com a tutela à liberdade de expressão, evitando-se atos arbitrários ou de censura prévia injustificada.

No ordenamento pátrio, o Marco Civil da Internet (Lei nº 12.965/2014) fixou o regime de guarda e disponibilização de dados, condicionando o fornecimento de registros e conteúdos à prévia ordem judicial (arts. 10 e 22). Complementando esse arcabouço, a Lei nº 15.211/2025 estipulou obrigações proativas aos provedores, tais como o dever de remoção imediata, a notificação formal às autoridades competentes em casos de aparente exploração sexual e a retenção temporária dos dados associados a essas notificações (art. 27).

A responsabilidade civil dos provedores por danos decorrentes de conteúdos gerados por terceiros também foi redefinida pelo STF no julgamento do Tema 533 da Repercussão Geral (SUPREMO TRIBUNAL FEDERAL, 2026), estabelecendo parâmetros para a responsabilização por inércia ou falha no dever de cuidado, sem afastar a reserva de jurisdição para a quebra de sigilo no processo penal.

4.2 Balizas legais para a obtenção de dados e a distinção de regimes jurídicos

A colheita probatória junto aos provedores de aplicação exige a observância rigorosa das categorias de dados estabelecidas pelo Marco Civil da Internet, evitando-se requisições genéricas ou em desconformidade com os regimes de proteção constitucional da intimidade e do sigilo das comunicações. O ordenamento jurídico estabelece três níveis distintos de proteção: os dados cadastrais, os registros de acesso (conexão e aplicação) e o conteúdo das comunicações privadas (BRASIL, 2014).

Os dados cadastrais — compreendidos estritamente como a qualificação pessoal, filiação e endereço do usuário (art. 10, § 3º, do MCI) — podem ser requisitados diretamente pela autoridade policial ou pelo Ministério Público sem a necessidade de prévia autorização judicial.

Sob outra perspectiva, o acesso aos registros de conexão e aos registros de aplicação submete-se à reserva de jurisdição (art. 22 do MCI), exigindo representação motivada que demonstre fundados indícios da infração e a utilidade estrita dos dados para a investigação, delimitando-se o período temporal pretendido (BRASIL, 2014). O nível máximo de tutela recai sobre o conteúdo de comunicações privadas, cujo fornecimento depende de ordem judicial fundamentada e do preenchimento dos requisitos da interceptação e quebra de sigilo (art. 10, § 2º, do MCI).

Na esfera investigativa, deve-se reforçar a distinção operada pela jurisprudência do Superior Tribunal de Justiça entre a preservação cautelar dos registros e a sua efetiva entrega às autoridades. Com amparo nos arts. 13, § 2º, e 15, § 2º, do Marco Civil da Internet, os órgãos de persecução penal podem ordenar administrativamente aos provedores a preservação imediata dos registros de rede para evitar a sua exclusão decorrente do decurso dos prazos legais de guarda.

Contudo, conforme assentou o STJ no AgRg no HC 998.395/SP, o requerimento de preservação não confere acesso aos dados, mantendo-se hígida a exigência de ordem judicial para a posterior disponibilização dos registros preservados (SUPERIOR TRIBUNAL DE JUSTIÇA, 2025a).

Além disso, nos cenários em que o compartilhamento de IPs via CGNAT impeça a individualização do terminal, torna-se indispensável a requisição da porta lógica de origem. Conforme decidido no REsp 2.170.872/SP (STJ), a indicação da porta lógica pela aplicação e pelo provedor de conexão viabiliza a identificação técnica do acesso, constituindo elemento fundamental para o prosseguimento das investigações de crimes de violência sexual infantojuvenil (SUPERIOR TRIBUNAL DE JUSTIÇA, 2025b).

4.3 Elementos de conexão da territorialidade e a incidência da jurisdição nacional

Um dos maiores entraves à persecução de crimes cibernéticos decorre da estrutura transnacional das plataformas digitais, cujas sedes corporativas e servidores de armazenamento frequentemente se situam fora do território brasileiro. Como salientam Reis e Jacob (2025), o embate histórico envolve alegações das big techs sobre ineficácia da jurisdição nacional, conflito de soberania ou entraves decorrentes do uso da criptografia de ponta a ponta e de legislações de privacidade dos seus países de origem.

O Marco Civil da Internet pacificou a matéria ao adotar no seu art. 11 a teoria dos elementos de conexão. A legislação estabelece que as leis brasileiras se aplicam obrigatoriamente a qualquer operação de coleta, armazenamento, guarda ou tratamento de dados por provedores, desde que ao menos um desses atos ocorra em território nacional, ou quando os serviços forem ofertados ao público brasileiro, ainda que por empresa estrangeira consorciada ou representada por filial no País (art. 11, §§ 1º e 2º, do MCI) (BRASIL, 2014).

A constitucionalidade dessa regra foi definitivamente confirmada pelo Supremo Tribunal Federal no julgamento da Ação Declaratória de Constitucionalidade nº 51 (ADC 51/DF). O Tribunal Pleno fixou o entendimento de que as autoridades judiciárias brasileiras possuem competência para determinar a requisição direta de dados e conteúdos mantidos por provedores de aplicação que prestam serviços no Brasil, ainda que os dados estejam armazenados em servidores localizados no exterior, sempre que presentes os elementos de conexão do art. 11 do Marco Civil ou do art. 18 da Convenção de Budapeste (SUPREMO TRIBUNAL FEDERAL, 2023).

Afasta-se, dessa maneira, a tese de que a simples localização física do servidor em solo estrangeiro impediria a incidência da jurisdição penal e da legislação processual brasileira.

4.4 A cooperação jurídica internacional e a aplicação da Convenção de Budapeste

Embora a ADC 51/DF tenha legitimado a requisição direta às filiais de provedores estrangeiros instaladas no Brasil, existem situações em que a prova digital se encontra sob o controle exclusivo de empresas ou servidores no exterior sem representação no País, ou em que a produção da prova dependa de diligências executadas em jurisdição estrangeira. Nesses casos, a morosidade e ineficácia das cartas rogatórias tradicionais impulsionaram a adesão do Brasil a instrumentos multilaterais para afastar cenários de impunidade.

O principal instrumento internacional para o enfrentamento da delituosidade cibernética no Brasil é a Convenção sobre o Crime Cibernético (Convenção de Budapeste),

promulgada pelo Decreto nº 11.491/2023 (BRASIL, 2023). O tratado internacional fornece balizas para a harmonização de tipos penais materiais, estabelece normas de direito processual para a obtenção de provas em meio eletrônico e institui canais céleres de assistência mútua entre os Estados-Partes.

Entre os mecanismos de cooperação previstos na Convenção de Budapeste, destaca-se a operacionalização da Rede de Contatos 24/7 (art. 35), que viabiliza a assistência imediata entre autoridades centrais para a preservação emergencial de dados eletrônicos e o auxílio técnico em investigações urgentes (BRASIL, 2023). A atuação via Rede 24/7 permite contornar a morosidade tradicional dos Tratados de Assistência Mútua em Matéria Penal (MLATs), garantindo que os registros de rede de crimes graves — como a exploração e o abuso sexual de crianças e adolescentes — sejam congelados preventivamente antes da sua exclusão definitiva.

Ressalte-se, contudo, que a preservação expedita facultada pela Convenção de Budapeste serve exclusivamente para assegurar a custódia temporária dos dados, não autorizando o repasse automático do seu conteúdo às autoridades investigantes sem o prévio envio e processamento do pedido formal de cooperação jurídica internacional e o preenchimento dos requisitos legais das jurisdições envolvidas (BRASIL, 2023). A articulação entre a requisição direta balizada pela ADC 51 e a utilização tempestiva dos canais da Convenção de Budapeste constitui, portanto, o caminho indispensável para superar os gargalos transnacionais da prova digital e garantir a punição efetiva dos agressores.

5 CONSIDERAÇÕES FINAIS

A adequação do modelo jurídico brasileiro de regulamentação das redes sociais e de persecução penal é uma realidade a ser enfrentada pelo Estado e pela sociedade no que tange à efetiva proteção de crianças e adolescentes contra crimes praticados no ambiente digital. O estudo demonstrou que, embora o ordenamento tenha avançado com a consolidação do dever geral de cuidado das plataformas (ECA Digital) e com novos instrumentos investigativos, a salvaguarda do princípio da proteção integral ainda esbarra em severos gargalos operacionais e normativos.

Inicialmente, o estudo tinha como hipótese a premissa de que o modelo jurídico brasileiro apresentava limitações relevantes na repressão a esses ilícitos, estando tais limitações relacionadas à dificuldade de identificação dos autores, à complexidade na produção e preservação da prova digital (cadeia de custódia), à dependência de cooperação com provedores

de aplicações frequentemente sediados no exterior e à necessidade de maior integração entre os órgãos responsáveis pela investigação e responsabilização penal.

No decurso da investigação, ao responder diretamente ao problema de pesquisa, alcançou-se como resultado a constatação de que a hipótese formulada foi confirmada, demonstrando que o modelo jurídico atua sob desafios práticos substanciais. Constatou-se que, embora o arcabouço normativo tenha avançado com a consolidação do dever geral de cuidado das plataformas (ECA Digital), a tipificação do cyberbullying (Lei nº 14.811/2024) e a instituição da ronda virtual (Lei nº 15.487/2026), a efetividade da persecução penal ainda esbarra na volatilidade das evidências eletrônicas, nas exigências técnicas da cadeia de custódia (arts. 158-A a 158-F do CPP) e na resistência corporativa ou morosidade na cooperação com big techs estrangeiras.

Por fim, o estudo deixa lacuna e oportunidade para investigações futuras a necessidade de acompanhar empiricamente a aplicação prática do ECA Digital pelas autoridades administrativas e judiciais, bem como aprofundar as pesquisas sobre o impacto do uso de inteligência artificial generativa na criação de conteúdos sintéticos ilícitos (deepfakes) contra a dignidade sexual de menores.

REFERÊNCIAS

ARAÚJO, Tuyanne Filgueiras Mendes. **Os desafios do Direito Penal na proteção das crianças e adolescentes na era digital**: uma análise da repressão dos crimes cibernéticos à luz da Lei 14.811/24. 2024. 69 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) — Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024. Disponível em: http://hdl.handle.net/11422/25324. Acesso em: 9 out. 2026.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, São Paulo, v. 29, n. 343, p. 7–9, 2021. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 9 out. 2026.

BADARÓ MASSENA, Caio. A propósito da cadeia de custódia das provas digitais no processo penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa. **Boletim IBCCRIM**, São Paulo, v. 31, n. 368, p. 19–21, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/506. Acesso em: 9 out. 2026.

BARBOSA, Carolina Tozi. **Crimes informáticos contra a dignidade sexual de crianças e adolescentes**: aspectos dogmáticos penais. 2024. 36 f. Trabalho de Conclusão de Curso (Graduação em Direito) — Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2024. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/43720. Acesso em: 9 out. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 9 out. 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 9 out. 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 9 out. 2026.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 9 out. 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 9 out. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 out. 2026.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 9 out. 2026.

BRASIL. **Lei nº 14.811, de 12 de janeiro de 2024**. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares e altera a legislação pertinente. Brasília, DF: Presidência da República, 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm. Acesso em: 9 out. 2026.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (ECA Digital). Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 9 out. 2026.

BRASIL. **Lei nº 15.487, de 6 de agosto de 2026**. Institui medidas de enfrentamento e repressão ao crime de violência sexual contra criança ou adolescente. Brasília, DF: Presidência da República, 2026d. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/L15487.htm. Acesso em: 9 out. 2026.

CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. *In*: CASTELLS, Manuel; CARDOSO, Gustavo (org.). **A sociedade em rede**: do conhecimento à acção política. Lisboa: Imprensa Nacional-Casa da Moeda, 2005. p. 17–30. Disponível em:

https://www.researchgate.net/publication/301788806_A_Sociedade_em_Rede_Do_Conhecimento_a_Accao_Politica. Acesso em: 9 out. 2026.

FERNANDES, Elora. Direitos de crianças e adolescentes por design: uma agenda regulatória para a ANPD. *In*: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (coord.). **Privacidade e proteção de dados de crianças e adolescentes**. Rio de Janeiro: ITS Rio; Obliq, 2021. p. 200–254. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2021/12/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes-its-1.pdf. Acesso em: 9 out. 2026.

FRAZÃO, Ana. **Parecer: dever geral de cuidado das plataformas diante de crianças e adolescentes**. [S. l.]: Instituto Alana, 2023. Disponível em: https://alana.org.br/material/parecer-ana-frazao/. Acesso em: 9 out. 2026.

JUNIOR, Aury L. Direito Processual Penal - 23ª Edição 2026. 23. ed. Rio de Janeiro: SRV, 2026. E-book. p.xiii. ISBN 9786551771675. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786551771675/. Acesso em: 20 out. 2026.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. 3. ed. São Paulo: Editora 34, 2010. Disponível em: https://ria.ufrn.br/jspui/handle/123456789/1874. Acesso em: 9 out. 2026.

PEIXOTO, Fabiano Hartmann; BUENO, Bárbara Nunes Ferreira; PEREIRA, João Sergio dos Santos Soares. Crianças e adolescentes: deveres de proteção e cuidado dos pais e responsáveis no ambiente digital. **Direito.UnB**: Revista de Direito da Universidade de Brasília, Brasília, v. 8, n. 1, p. 181–214, 2024. DOI: https://doi.org/10.26512/2357-80092024e47390.

REIS, Lucas Gabriel Rocha Mamede; JACOB, Alexandre. A proteção aos menores contra crimes cibernéticos: responsabilidade penal e o papel das plataformas digitais. **Revista Multidisciplinar do Nordeste Mineiro (REMUNOM)**, [s. l.], v. 19, n. 3, p. 1–12, 2025. DOI: https://doi.org/10.61164/87wgex31.

SAAD GIMENES, Marta C.; ROSSI, Helena C.; PARTATA, Pedro H. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 10, n. 3, e1071, set./dez. 2024. DOI: https://doi.org/10.22197/rbdpp.v10i3.1071.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet**: construção e aplicação. Juiz de Fora: Editar, 2016. Disponível em: https://civilistica.emnuvens.com.br/redc/article/download/495/525/1475. Acesso em: 9 out. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Agravo Regimental no Habeas Corpus nº 998.395/SP**. Relator: Ministro Ribeiro Dantas. Quinta Turma, julgamento em 13 ago. 2025. *Diário da Justiça Eletrônico Nacional*, Brasília, DF, 18 ago. 2025a. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&O=RR&preConsultaPP=000007630%2Fo&thesurus=JURIDICO&p=true&tp=T. Acesso em: 9 out. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial nº 2.170.872/SP**. Relatora: Ministra Nancy Andrighi. Terceira Turma, julgamento em 18 mar. 2025. *Diário da Justiça Eletrônico*

Nacional, Brasília, DF, 21 mar. 2025b. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&O=RR&preConsultaPP=7027/0&thesaurus=JURIDICO&p=true&tp=T. Acesso em: 9 out. 2026.

SUPREMO TRIBUNAL FEDERAL. **Ação Declaratória de Constitucionalidade nº 51/DF**. Relator: Ministro Gilmar Mendes. Tribunal Pleno, julgamento em 23 fev. 2023. Brasília, DF: Supremo Tribunal Federal, 2023. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5328854. Acesso em: 9 out. 2026.

SUPREMO TRIBUNAL FEDERAL. **Recurso Extraordinário nº 593.727/MG**. Relator originário: Ministro Cezar Peluso; redator do acórdão: Ministro Gilmar Mendes. Tribunal Pleno, julgamento em 14 maio 2015. Tema 184 da repercussão geral. Brasília, DF: Supremo Tribunal Federal, 2015. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=2636585&numeroTema=184. Acesso em: 9 out. 2026.

SUPREMO TRIBUNAL FEDERAL. **Recurso Extraordinário nº 1.057.258/MG**. Relator: Ministro Luiz Fux. Tribunal Pleno. Tema 533 da repercussão geral. Julgamento de mérito concluído em 26 jun. 2025. Brasília, DF: Supremo Tribunal Federal, 2026b. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?classeProcesso=RE&incidente=5217273&numeroProcesso=1057258&numeroTema=533. Acesso em: 9 out. 2026.

UNITED NATIONS. Committee on the Rights of the Child. **General comment No. 25 (2021) on children's rights in relation to the digital environment**. Geneva: United Nations, 2021. Documento CRC/C/GC/25. Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em: 9 out. 2026

VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. **The platform society**: public values in a connective world. New York: Oxford University Press, 2018. Disponível em: https://www.semanticscholar.org/paper/The-Platform-Society%3A-Public-Values-in-a-Connective-Plantin-Dijck/25133a6c7627c9bc070d57928417506f39035c4a. Acesso em: 9 out. 2026.