SECRETARIA NACIONAL DE DIREITOS DIGITAIS | JANEIRO 2026

MECANISMOS DE AFERIÇÃO DE IDADE

Análise das Contribuições à Consulta Pública e Subsídios para Regulamentação da Lei nº 15.211/2025

CRESCER EM PAZ
ESTRATÉGIA DE JUSTIÇA E SEGURANÇA PÚBLICA PARA PROTEÇÃO DE CRIANÇAS E ADOLESCENTES

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Ministério da Justiça e Segurança Pública

Secretária Nacional de Direitos Digitais
Lílian Cintra de Melo

Equipe técnica da Secretaria Nacional de Direitos Digitais
Ricardo de Lins e Horta
Ediane de Assis Bastos
Eduardo de Araújo Nepomuceno
Carlos Frederico Carvalho Redmond Fortes
João Victor Soares Simões
Mariana Gomes de Barros Fernandes Tavora
Kamilla Mariana Martins Rodrigues

Consultora técnica
Professora Ticianne de Góis Ribeiro Darin - Universidade Federal do Ceará (UFC)
Organização das Nações Unidas para a Educação, Ciência e Cultura (UNESCO)

Demais membros do Comitê Consultivo para a Formulação de Proposta de Metodologia e Requisitos Mínimos de Verificação Etária (Portaria MJSP n° 925/2025)

Subsecretaria de Tecnologia da Informação da Secretaria-Executiva do MJSP
José Rocha de Carvalho Filho
Monica Mattos Pellegrini

Secretaria Nacional do Consumidor
Giuliana Tomassini Melo
Angelica Lopes Amaro

Agência Nacional de Proteção de Dados
Jorge Andre Ferreira Fontelles de Lima
Rodrigo Santana dos Santos

Organizações da sociedade civil ou especialistas de reconhecida atuação no tema
Helena Secaf – Coalizão Direitos na Rede
Luciana Temer – Instituto Liberta
Maria Mello – instituto Alana
Vanessa Cavalieri - Juíza da Vara da Infância do Tribunal de Justiça do Rio de Janeiro
Yasodara Córdova - Pesquisadora

Data de publicação
Janeiro de 2026

Como citar
BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Direitos Digitais. *Mecanismos de aferição de idade. Análise das Contribuições à Consulta Pública e Subsídios para Regulamentação da Lei nº 15.211/2025.* Brasília: MJSP, janeiro de 2026.

AGRADECIMENTOS

Este relatório foi desenvolvido conjuntamente pela equipe da Secretaria Nacional de Direitos Digitais do Ministério da Justiça e Segurança Pública e pela Profa. Dra. Ticianne Darin, da Universidade Federal do Ceará. Agradecemos à Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) pela parceria que viabilizou a elaboração do trabalho, bem como à Agência Nacional de Proteção de Dados (ANPD), cuja interlocução foi fundamental para o amadurecimento do estudo. Registramos, por fim, nosso reconhecimento às instituições e aos cidadãos que participaram da Consulta Pública na plataforma Participa + Brasil, cujas contribuições fundamentaram a análise aqui apresentada. Os subsídios coletados são essenciais para a definição dos padrões nacionais de aferição de idade, permitindo que a regulamentação incorpore a experiência técnica, as preocupações sociais e as visões de diferentes setores da sociedade brasileira. A pluralidade de posições reflete a complexidade do desafio de proteger crianças e adolescentes no ambiente digital, respeitando direitos fundamentais como a privacidade e a liberdade de expressão. Este documento busca honrar essa diversidade ao sistematizar os argumentos de forma equilibrada e transparente, fornecendo base sólida para as decisões regulatórias que se seguirão.

Lílian Cintra de Melo
Secretária Nacional de Direitos Digitais

ÍNDICE

NOTA METODOLÓGICA SOBRE REPRESENTATIVIDADE DA AMOSTRA

O presente relatório sistematiza as contribuições recebidas durante a Consulta Pública sobre Aferição de Idade na Internet Brasileira, realizada por meio da plataforma Participa + Brasil. Cumpre esclarecer aspectos metodológicos relevantes para a adequada interpretação dos resultados.

O universo de 70 contribuições analisadas constitui uma **amostra de conveniência**, resultante do processo de adesão voluntária dos participantes ao procedimento consultivo. Como tal, **não possui representatividade estatística** do universo de stakeholders afetados pela regulação da aferição de idade no Brasil. Os resultados refletem exclusivamente as posições dos atores que optaram por participar da consulta, não sendo extrapoláveis para o conjunto da população

A análise revela concentrações significativas que devem ser consideradas na interpretação dos dados:

- **Concentração Setorial:** O setor privado responde por 41,4% das contribuições, seguido pela sociedade civil (34,3%). A academia contribuiu com apenas 4,3% das manifestações, o que pode resultar em sub-representação de perspectivas técnico-científicas independentes.

- **Concentração Geográfica:** A região Sudeste concentra 54,3% das contribuições, percentual superior à soma de todas as demais regiões. Essa concentração está correlacionada à localização das sedes das empresas participantes (69% do setor privado). As regiões Norte e Sul apresentam as menores frequências relativas, o que pode implicar lacunas na representação de perspectivas regionais específicas.

- **Participação Internacional:** As 6 contribuições internacionais (8,6%) são quase exclusivamente de natureza empresarial (5 do setor privado) e provenientes dos Estados Unidos e Reino Unido, refletindo a inserção de empresas transnacionais no mercado brasileiro, sem representação de outras regiões do Sul Global.

Em observância à Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e aos princípios de privacidade que fundamentam a própria consulta, as contribuições de pessoas físicas foram anonimizadas neste relatório, sendo referenciadas pela categoria "Contribuinte – Sociedade Civil" ou equivalente. As citações diretas de manifestações individuais foram mantidas apenas quando estritamente necessárias para ilustrar argumentos paradigmáticos, sem identificação nominal dos autores.

Os resultados apresentados devem ser interpretados como um mapeamento qualitativo dos argumentos mobilizados pelos atores participantes, e não como um levantamento exaustivo ou estatisticamente representativo das posições existentes no debate público. A ausência de determinados argumentos ou perspectivas no corpus analisado não implica sua inexistência ou irrelevância no debate mais amplo sobre aferição de idade.

A SEDIGI reconhece essas limitações e reafirma o compromisso de complementar os subsídios da consulta pública com outras formas de interlocução institucional, pesquisas técnicas independentes e diálogo com segmentos sub-representados na presente amostra, incluindo comunidades indígenas e quilombolas, crianças em acolhimento institucional, e representantes de regiões com menor participação no processo consultivo.

As posições, argumentos e modelos descritos neste relatório refletem a interpretação da equipe técnica da SEDIGI sobre as contribuições recebidas na Consulta Pública. A categorização de contribuintes por setor e a síntese de seus argumentos foram realizadas para fins analíticos, não constituindo validação ou endosso das posições apresentadas.

1. SUMÁRIO EXECUTIVO

1.1 Sobre a tomada de subsídios

Este relatório é apresentado como resultado da Consulta Pública sobre Aferição de Idade na Internet Brasileira, elaborada pela Secretaria Nacional de Direitos Digitais (SEDIGI) do Ministério da Justiça e Segurança Pública em colaboração com a Agência Nacional de Proteção de Dados (ANPD), estabelece as diretrizes para a regulamentação dos mecanismos de aferição de idade previstos na Lei n° 15.211/2025 (Estatuto Digital da Criança e do Adolescente - ECA Digital). A consulta integra a estratégia "Crescer em Paz" e visa coletar subsídios técnicos e sociais para implementar um sistema de garantia de idade (*age assurance*) que equilibre a proteção integral de crianças e adolescentes com a preservação da privacidade e dos dados pessoais dos usuários. O texto fundamenta-se na premissa de que a "aferição de idade" difere da "verificação de identidade", devendo limitar-se à confirmação do atributo de idade mínima autorizada (resposta binária sim/não) sem a necessidade de identificar civilmente o usuário ou monitorar seu comportamento, em estrita observância aos princípios da necessidade e finalidade da Lei Geral de Proteção de Dados (LGPD).

A análise das contribuições indica convergência em torno de uma abordagem baseada no risco e na proporcionalidade, rejeitando a autodeclaração como método válido para serviços de alto risco. Contribuintes propuseram diferentes classificações de métodos técnicos conforme critérios de eficácia e intrusividade. Diversos participantes indicaram preferência pelo uso de infraestruturas de Identidade Digital, como carteiras digitais (*wallets*) com credenciais verificáveis e provas de conhecimento zero (*zero knowledge proof* - ZKP), e soluções de *Open Banking*, que minimizam a exposição de dados. Em contrapartida, organizações da sociedade civil e da academia que participaram da consulta expressaram cautela quanto a métodos baseados em biometria facial devido aos riscos de vigilância, vieses algorítmicos e coleta excessiva de dados sensíveis. A arquitetura proposta sugere um modelo de responsabilidade compartilhada em "dupla camada": uma verificação estrutural no nível dos sistemas operacionais e lojas de aplicativos (fornecendo um "sinal de idade" genérico) e uma

verificação pontual e robusta realizada diretamente pelas aplicações em casos de alto risco ou conteúdo restrito a maiores de 18 anos.

O texto também mapeia as diferentes abordagens identificadas nas contribuições do setor empresarial em relação à implementação de proteções proativas (*safety by design*). Enquanto algumas plataformas de redes sociais propuseram modelos baseados em análise comportamental pós-acesso, o documento registra também propostas de barreiras preventivas. Setores como jogos eletrônicos e *marketplaces* levantam preocupações sobre fricção e usabilidade, enquanto a indústria de conteúdo adulto aponta riscos de migração de usuários para mercados não regulados. Por fim, são elencados desafios estruturais para a implementação no cenário brasileiro, incluindo o risco de aprofundamento da exclusão digital devido às limitações de hardware da população, a complexidade da verificação em dispositivos compartilhados por famílias e a necessidade de governança em arquiteturas descentralizadas. A consulta busca, portanto, definir critérios de certificação e padrões de interoperabilidade que garantam a eficácia da lei sem criar barreiras de acesso ou vulnerabilidades de segurança.

1.2 Perfil dos participantes

A caracterização dos setenta participantes do processo de consulta revela uma estrutura de representação predominantemente constituída por agentes do setor privado e da sociedade civil, articulada a uma distribuição geográfica caracterizada pela concentração na região Sudeste. A análise da variável institucional indica que o Setor Privado responde pela maior fatia das contribuições, totalizando 29 registros (41,4%), seguido pela sociedade civil, com 24 entradas (34,3%). A soma destes dois segmentos estabelece uma preponderância de interesses corporativos e associativos sobre a participação direta de entes estatais, classificados como Poder Público (5 registros), e instituições de ensino e pesquisa, categorizadas como Academia (3 registros).

No âmbito geográfico, observa-se uma assimetria na origem das submissões. A região Sudeste concentra 38 contribuições, perfazendo 54,3% do total, um volume superior à soma de todas as outras macrorregiões nacionais e internacionais. O Centro-Oeste e o Nordeste apresentam representatividade intermediária, com 11 e 8

participantes respectivamente, enquanto as regiões Sul (5) e Norte (2) figuram com as menores frequências absolutas no território nacional. A dimensão internacional é composta por 6 participantes, oriundos dos Estados Unidos e do Reino Unido, cuja natureza institucional é quase exclusivamente privada. O cruzamento das variáveis evidencia que a centralidade geográfica no Sudeste está diretamente correlacionada à localização das sedes das empresas participantes, visto que 69% do contingente do setor privado origina-se desta região, ao passo que a sociedade civil demonstra uma dispersão territorial comparativamente superior.

1.3 Eixos temáticos

A análise transversal das contribuições revela que o debate sobre aferição de idade no Brasil vai além da definição técnicas de que métodos utilizar. A análise sugere que o debate envolve não apenas aspectos técnicos, mas também questões sobre custódia de dados e atribuição de responsabilidades dos usuários e quem deve responder judicialmente por eventuais falhas. Observou-se que diferentes atores propuseram modelos que distribuem responsabilidades de formas distintas ao longo da cadeia de valor: os provedores de conteúdo argumentam que a tarefa caberia às lojas de aplicativos, as lojas sustentam que a responsabilidade seria dos desenvolvedores, e diferentes atores propõem que o dever de fiscalização seja compartilhado com as famílias ou exercido pelo Estado. O presente relatório descreve uma visão panorâmica dos dados e participantes e, em seguida, detalha a complexidade do debate através de nove eixos temáticos que correspondem às categorias analíticas emergentes.

Eixo 1: Diagnóstico e atribuição de responsabilidade

O primeiro eixo examina a base ética da regulação. Existe um consenso entre os participantes de que os atuais métodos de autodeclaração (como clicar em “tenho mais de 18 anos”) para produtos e conteúdos proibidos falharam e são facilmente burlados por crianças. A divergência surge na definição de quem deve corrigir essa falha. Parte dos contribuintes do setor privado argumentou que a segurança digital envolve primordialmente o dever de supervisão dos pais, cabendo às empresas fornecer ferramentas de apoio à supervisão parental. Em contrapartida, a organizações da sociedade civil e da academia defendem a responsabilidade

solidária, afirmando que as empresas criam o risco e, portanto, devem ter o dever objetivo de mitigá-lo, não podendo terceirizar essa função para famílias sem conhecimento técnico. Os provedores de conteúdo utilizam o termo “devida diligência” para defender que sua obrigação, em caso de produtos e serviços não proibidos por lei para menores de 18 anos, deve ser a de empregar “melhores esforços”, e não de garantia de resultado. Uma minoria dos contribuintes questiona a própria existência do problema, sugerindo que a regulação responde a questionamentos sobre a base empírica dos danos alegados.

Eixo 2: Escopo e definição do objeto regulado

O segundo eixo delimita o perímetro de aplicação da norma, evidenciando uma disputa ontológica sobre a natureza do risco. Contribuintes do setor privado, em sua maioria, advogaram por, limitando a obrigatoriedade de verificação robusta a conteúdos proibidos por lei, especificamente pornografia e jogos de azar, excluindo redes sociais. Organizações da sociedade civil que participaram da consulta, inversamente, propõe uma definição baseada no risco estrutural e no design comportamental, utilizando critérios como a interação entre desconhecidos e algoritmos de recomendação para classificar serviços. Como mecanismo de mediação, surge a proposta de uma matriz de risco escalonada. Simultaneamente, observa-se um movimento de setores específicos -- financeiro, editorial e plataformas profissionais -- que reivindicam isenções totais ou parciais, alegando o cumprimento prévio de normas (como *Know Your Customer*) ou a natureza não nociva das suas atividades. Há também uma defesa de que a lei foque apenas nos “*gatekeepers*”, isentando pequenos desenvolvedores para não sufocar a inovação.

Eixo 3: Arquitetura de implementação

O terceiro eixo trata da geopolítica da infraestrutura, questionando onde, na cadeia de valor da internet, a verificação deve ocorrer. Identifica-se uma tensão entre modelos de centralização nas lojas de aplicações e sistemas operacionais, defendidos por fornecedores de conteúdo para evitar a fricção, e modelos de descentralização ao nível da aplicação, defendidos por fabricantes de hardware sob a alegação de cegueira contextual da infraestrutura. A realidade sociológica brasileira dos dispositivos partilhados desafia a viabilidade de modelos baseados num cadastro

único no dispositivo, uma vez que a identidade do proprietário do *hardware* frequentemente não corresponde à do usuário momentâneo. Este fato sustenta demandas mais rigorosas pela verificação a cada acesso, embora tal exigência enfrente resistência devido à complexidade da cadeia de responsabilidade e à dificuldade de imputar controle a intermediários como anunciantes.

Eixo 4: Soluções técnicas e métodos

O quarto eixo analisa as ferramentas propostas. Contribuintes do setor privado apontam para estimativa facial e comportamental por inteligência artificial, vendendo-as como soluções rápidas que não exigem documentos físicos. Organizações da sociedade civil manifestaram preocupações quanto a essa tecnologia por considerá-la invasiva e propõe o uso de ZKP (*tokens* criptográficos), que provam a idade sem revelar a identidade. O uso da infraestrutura do Gov.br aparece como uma alternativa de validação central, mas enfrenta resistência tanto daqueles que temem monopólio estatal, quanto daqueles que temem vigilância. Outras opções debatidas incluem o uso de dados bancários, o envio de documentos digitalizados e a autodeclaração reforçada para casos de menor risco.

Eixo 5: Argumentos de Legitimação

O quinto eixo agrupa os argumentos utilizados pelos contribuintes para fundamentar suas posições regulatórias. Contribuintes do setor regulado apresentaram argumentos de conformidade prévia e destacaram o valor social de suas plataformas. A tecnologia de estimativa facial foi defendida por alguns contribuintes como ferramenta de inclusão, por dispensar documentos oficiais.

Eixo 6: Adequação e proporcionalidade

O sexto eixo estabelece os princípios calibradores da regulação. O consenso aponta para a necessidade de uma abordagem proporcional, onde o alto risco exige rigor na verificação e o baixo risco permite flexibilidade. O princípio da minimização de dados emerge como a regra fundamental para a adequação de qualquer solução técnica, favorecendo arquiteturas que não armazenam informações pessoais. Contudo, reconhece-se que a solução tecnológica é insuficiente se não for acompanhada de políticas de educação midiática. A análise aponta ainda para a

necessidade de mecanismos de inclusão *offline*, garantindo que cidadãos sem acesso a dispositivos sofisticados possam realizar a aferição de idade através de meios físicos ou assistidos.

Eixo 7: Riscos específicos a direitos

O sétimo eixo detalha as externalidades negativas associadas à privacidade e segurança. Existe um temor estrutural quanto à criação de *honeypots* de dados biométricos, que centralizam informações sensíveis e atraem ataques cibernéticos. O risco de vigilância estatal e o uso da infraestrutura de verificação para controle social ou político são preocupações prementes, assim como a mineração comercial de dados e a reidentificação cruzada de usuários. Um risco específico emergente é o desvio de finalidade das imagens recolhidas para o treino de modelos de inteligência artificial sem consentimento. Adicionalmente, questiona-se a eficácia técnica das medidas devido à facilidade de evasão através de VPNs e contas falsas, o que poderia tornar a regulação ineficaz.

Eixo 8: Impactos e barreiras socioeconômicas

O oitavo eixo aborda as consequências econômicas e sociais da regulação. A imposição de custos elevados de conformidade é identificada como uma barreira para pequenas e médias empresas, podendo induzir a uma maior concentração de mercado em torno das grandes empresas de tecnologia. O repasse destes custos ao consumidor final é uma externalidade prevista. No plano social, o risco de exclusão digital é visto como significativo, dado que uma parcela da população possui dispositivos obsoletos ou carece de literacia familiar para configurar ferramentas de controle parental. Surge o argumento de que a excessiva fricção no uso pode levar ao abandono de serviços legítimos ou à migração para um mercado paralelo não regulado. Considera-se também o impacto na autonomia juvenil, especialmente para adolescentes entre 16 e 17 anos, e as dificuldades práticas de fiscalização estatal perante o volume de tráfego digital.

Eixo 9: Desenho regulatório e governança

O nono e último eixo temático consolida as propostas regulamentação sugeridas. Parte do setor privado requer maior clareza nas orientações e definições para garantir segurança jurídica, bem como prazos de adaptação realistas, criticando a complexidade burocrática. A solução de governança proposta envolve a criação de sistemas de certificação e auditoria pública para validar a segurança das ferramentas de verificação, evitando a autoavaliação pelas plataformas. O uso de *sandboxes* regulatórios é apontado como um caminho consensual para testar tecnologias em ambiente controlado antes da obrigatoriedade geral. Por fim, defende-se a adoção de interfaces de programação (APIs) abertas e a harmonização com padrões internacionais para garantir a interoperabilidade e a neutralidade tecnológica, evitando que a regulação favoreça monopólios tecnológicos específicos.

1.4 Síntese das tensões identificadas

A. Proteção *versus* vigilância

Identifica-se um tensão significativa que demanda mediação regulatória sobre os métodos de verificação que permitem a identificação, onde as soluções propostas para a proteção da infância são percebidas por alguns atores como potenciais vetores de vigilância. Contribuintes do setor privado defendem a adoção de estimativa facial e biometria como ferramentas de inclusão social para usuários sem documentação, argumento que é contestado por organizações da sociedade civil e academia, que apresentam preocupações levantadas por contribuintes sobre a segurança de bases de dados biométricos suscetíveis a ataques cibernéticos (*honeypots*) e permitem o desvio de finalidade para o treinamento não autorizado de Inteligência Artificial. A proposta de centralização da verificação na infraestrutura governamental (Gov.br) gera uma convergência quanto à rejeição à custódia estatal da identidade, seja por temor de ineficiência e monopólio, ou pelo risco de monitoramento estatal do comportamento online dos cidadãos e rastreamento de dissidentes.

B. Viabilidade econômica *versus* segurança técnica

Estabelece-se o desafio de equilíbrio entre a necessidade de robustez técnica e a realidade socioeconômica do mercado brasileiro. O setor privado apresenta dados sobre os custos de validação individual para sustentar que a exigência de métodos determinísticos (checagem de documentos) inviabilizaria a operação de pequenas e médias empresas, favorecendo a concentração de mercado em grandes empresas. Concomitantemente, o argumento da exclusão digital foi apresentado com base na obsolescência do parque tecnológico (dispositivos com câmeras de baixa resolução) e nos diferentes níveis de competência digital das famílias, para sustentar a manutenção de métodos de baixo atrito. Em contrapartida, a sociedade civil demanda a adoção de arquiteturas de preservação de privacidade, especificamente ZKP, que eliminariam a coleta de dados, mas que são rejeitadas pelo mercado sob a alegação de complexidade técnica e custo proibitivo. Identificou-se um desafio de conciliação entre soluções tecnicamente robustas, economicamente viáveis e politicamente aceitáveis, o que demanda abordagem incremental e experimentação regulatória.

C. Centralização infraestrutural *versus* responsabilidade contextual

A análise evidencia divergências sobre o ponto da cadeia de valor em que o controle de identidade deve ocorrer. Empresas globais de conteúdo defendem a verificação no nível da loja de aplicativos ou sistema operacional, argumentando que a centralização evita a redundância na coleta de dados e reduz a fricção para o usuário. Essa proposta é combatida pelos fabricantes de hardware e desenvolvedores de sistemas operacionais, que alegam “cegueira contextual”: a infraestrutura não possui capacidade de discernir se o uso de um aplicativo é nocivo ou educativo, o que exigiria uma verificação descentralizada no nível do aplicativo. Adicionalmente, a sociedade civil e a academia introduzem o argumento da soberania infraestrutural, alertando que a dependência de APIs de verificação fornecidas por conglomerados tecnológicos estrangeiros constitui uma vulnerabilidade de segurança nacional, defendendo a criação de emissores raiz nacionais e interoperáveis para evitar a dependência tecnológica de infraestruturas estrangeiras na gestão da identidade civil.

D. Ilegalidade manifesta *versus* risco estrutural

Observa-se uma divergência ontológica na definição do objeto a ser regulado, a partir do que é considerado como risco. Contribuintes do setor privado propuseram uma classificação de risco focada em categorias de ilegalidade manifesta. Sob essa ótica, redes sociais e plataformas de *streaming* são classificadas como serviços de baixo risco, aptos a regimes de autodeclaração ou inferência comportamental. Em oposição, a sociedade civil fundamenta a necessidade de regulação no conceito de risco estrutural derivado do design persuasivo e da economia da atenção, argumentando que mecanismos de engajamento viciante e coleta massiva de dados constituem ameaças ao desenvolvimento infantil tão graves quanto o conteúdo ilegal. Essa tensão define o perímetro de aplicação da norma: contribuintes do setor privado propuseram tratamento diferenciado para determinados modelos de negócio, enquanto a sociedade civil exige que a proporcionalidade da verificação seja calibrada pelo poder de influência da plataforma, e não apenas pela natureza do conteúdo hospedado.

1.5 Síntese das propostas identificadas nas contribuições

A análise das contribuições permitiu identificar propostas recorrentes que podem subsidiar a elaboração da regulamentação infralegal. Elas são apresentadas a seguir organizadas por eixo temático, refletindo os argumentos dos contribuintes.

A. Propostas relativas ao escopo de aplicação (ilegalidade vs. risco estrutural)

Contexto: Contribuintes divergiram sobre a extensão do mandato de verificação -- se restrito a conteúdos ilegais ou ampliado para riscos estruturais.

Propostas identificadas:

- **Abordagem escalonada por níveis de risco:** Em vez de regra binária (verifica/não verifica), diversos contribuintes propuseram o estabelecimento de níveis de exigência proporcionais ao potencial de dano do serviço. As faixas sugeridas incluem: (i) **risco crítico**, como conteúdo adulto e apostas, com verificação determinística; (ii) **risco elevado**, como redes sociais com algoritmos de recomendação, com

estimativa de idade ou verificação parental; (iii) **risco baixo**, como jogos sem interação social e comércio eletrônico, com autodeclaração reforçada.

- **Regulação do design, não apenas do acesso:** Para plataformas de risco intermediário, contribuintes da sociedade civil propuseram que a verificação de idade funcione como gatilho para ativação de configurações protetivas (desativação de publicidade direcionada, restrição de mensagens diretas com desconhecidos), em vez de resultar em bloqueio total de acesso.

B. Propostas relativas à arquitetura de implementação (centralização vs. contexto)

Contexto: Contribuintes divergiram sobre o ponto da cadeia de valor em que a verificação deve ocorrer -- se centralizada em lojas de aplicativos/sistemas operacionais ou descentralizada no nível das aplicações.

Propostas identificadas:

- **Modelo de responsabilidade em camadas:** Contribuintes de diferentes setores propuseram rejeitar a escolha binária entre loja e aplicativo, estabelecendo modelo híbrido no qual a infraestrutura (loja/sistema operacional) fornece "sinal de confiança" (*token* indicativo de verificação prévia) e a aplicação aplica as restrições contextuais específicas ao seu conteúdo.
- **Tratamento de dispositivos compartilhados:** Considerando a realidade brasileira de compartilhamento familiar de dispositivos, contribuintes propuseram que serviços de alto risco exijam revalidação em momentos-chave de uso, não se limitando à verificação única no momento do download.

C. Para a tensão de privacidade (proteção vs. vigilância)

Contexto: Contribuintes expressaram preocupações quanto ao risco de que a infraestrutura de verificação seja utilizada para vigilância ou exploração comercial de dados.

Propostas identificadas:

- **Limitação de finalidade**: Contribuintes da sociedade civil e parte do setor privado propuseram vedação expressa ao uso de dados coletados para verificação de idade para finalidades diversas, incluindo treinamento de modelos de inteligência artificial, perfilamento publicitário e compartilhamento com autoridades de segurança pública (salvo ordem judicial específica).
- **Arquitetura de preservação de privacidade**: Contribuintes propuseram o fomento a modelos de verificação que garantam separação de conhecimento, nos quais o verificador conhece a identidade, mas desconhece o destino do usuário, enquanto a plataforma conhece a faixa etária mas desconhece a identidade civil.

D. Propostas relativas à viabilidade econômica (viabilidade vs. segurança)

Contexto: Contribuintes do setor privado manifestaram preocupação com custos de conformidade e impactos sobre pequenas e médias empresas.

Propostas identificadas:

- **Assimetria regulatória**: Contribuintes propuseram que grandes plataformas arquem com custos de implementação de tecnologias robustas e disponibilizem interfaces de programação (APIs) acessíveis para o ecossistema, enquanto pequenas empresas tenham acesso a soluções públicas de baixo custo ou regimes simplificados.

- **Padronização de protocolos**: Contribuintes propuseram que o Estado defina requisitos mínimos e protocolos de interoperabilidade, permitindo que múltiplos fornecedores compitam para oferecer soluções de verificação, desde que observem padrões de privacidade estabelecidos.

E. Propostas relativas à governança

Contexto: Contribuintes de diferentes setores demandaram mecanismos de certificação e supervisão para garantir a confiabilidade das soluções de verificação.

Propostas identificadas:

- **Auditoria independente:** Contribuintes propuseram que empresas que utilizem estimativa facial ou inferência comportamental publiquem relatórios de impacto e submetam seus sistemas as avaliações de viés por terceiros independentes.
- **Regime de certificação:** Contribuintes propuseram a criação de programa de acreditação para provedores de tecnologia de verificação de idade, com incentivos para plataformas que contratem verificadores certificados.
- **Regime regulatório:** Houve convergência entre setores quanto à adoção de ambientes de teste controlados para experimentação de soluções antes da obrigatoriedade geral.

2. INTRODUÇÃO

2.1 Metodologia de análise de dados

O protocolo metodológico adotado para o exame das contribuições submetidas à plataforma “Participa + Brasil” fundamentou-se em uma abordagem híbrida, integrando procedimentos indutivos e dedutivos de análise qualitativa. Inicialmente, procedeu-se a uma análise indutiva, caracterizada pela leitura sistemática do conjunto de contribuições (formulários estruturados e arquivos PDF), permitindo que as categorias analíticas emergissem diretamente dos dados empíricos, sem a imposição apriorística de hipóteses teóricas. Esta fase exploratória resultou na construção de uma categorias analíticas que organizam os principais temas do debate regulatório.

Subsequentemente, aplicou-se uma análise dedutiva visando a identificação sistemática e a codificação das unidades de conteúdo. Definem-se aqui unidades de conteúdo como os segmentos semânticos mínimos — variando de sintagmas a parágrafos completos — que portam um sentido argumentativo, descritivo ou normativo autônomo e relevante para o objeto da consulta.

A operacionalização técnica deste processo utilizou o software *QualCoder*, uma ferramenta de código aberto para Análise Qualitativa de Dados Assistida por Computador (CAQDAS). A plataforma permitiu a segmentação precisa dos textos e a atribuição de códigos conforme os critérios estabelecidos. A interpretação foi organizada em três níveis de interpretação:

1. **Análise Intra-código:** Exame da consistência interna e das variações semânticas dentro de cada etiqueta individual, mapeando a frequência e a intensidade dos argumentos.

2. **Análise Inter-códigos:** Avaliação das relações lógicas (complementaridade, contradição, causalidade) entre os diferentes códigos pertencentes à mesma categoria analítica.

3. **Análise Inter-categorias:** Integração transversal dos dados para identificar tensões estruturais e macro-narrativas que atravessam os diferentes eixos temáticos.

A transposição das categorias analíticas resultantes para os nove eixos temáticos que estruturam este relatório reflete a complexidade reticular do debate. Embora estes eixos possuam categorias inter-relacionadas – admitindo que uma mesma unidade de conteúdo, como a menção a uma tecnologia biométrica, seja codificada simultaneamente em múltiplas categorias (por exemplo, como uma solução técnica e, concomitantemente, como um risco de vigilância) –, a interpretação conferida em cada Eixo é específica e orientada pela perspectiva específica de cada eixo. Ressalta-se, por fim, que a análise apresentada sistematiza a totalidade das unidades de conteúdo extraídas do *corpus*. A inserção de citações diretas ao longo do texto obedece estritamente a critérios de representatividade paradigmática dos argumentos centrais mobilizados pelos atores mais significativos. Portanto, a ausência de transcrição literal de determinadas contribuições não implica seu descarte, mas sim sua incorporação na síntese analítica dos argumentos coletivos que compõem a interpretação integral dos eixos.

Para garantir a replicabilidade e a consistência metodológica, foi desenvolvido um *Codebook* (Livro de Códigos), que atua como o glossário estruturante da análise, delimitando as definições operacionais, critérios de inclusão e exclusão para cada categoria e código, conforme detalhado na Tabela 1 (Anexo A).

2.3 Atores envolvidos

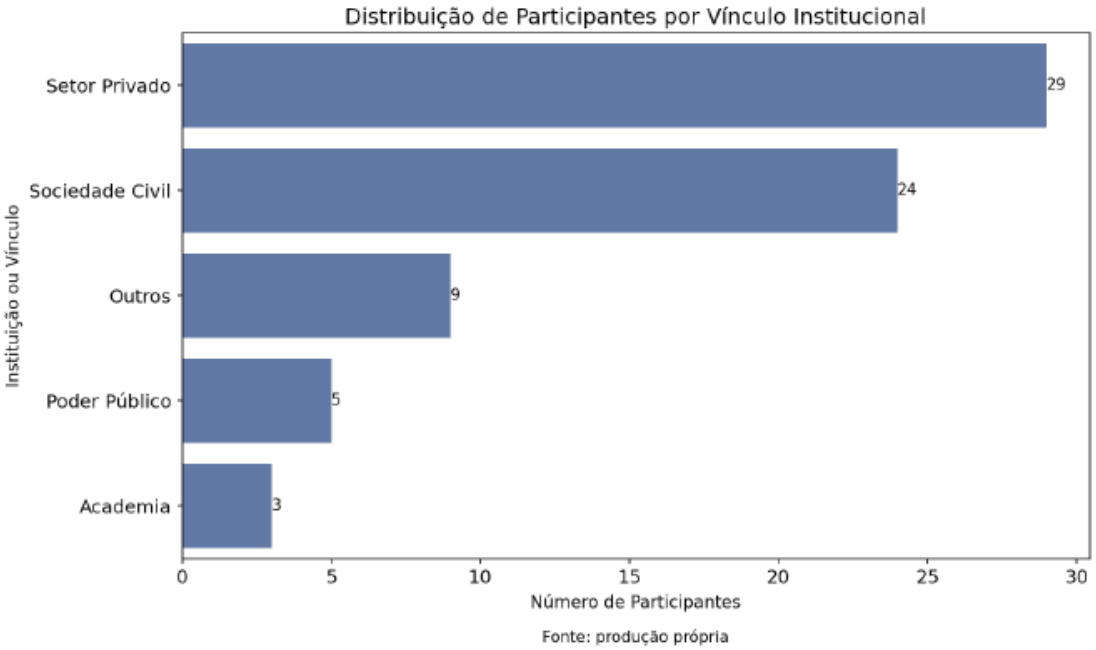
Análise da distribuição institucional dos participantes

O exame da variável referente ao vínculo institucional revela uma segmentação clara entre os atores envolvidos, com predominância numérica de entidades privadas e da sociedade civil organizada.

A categoria “Setor Privado” constitui o agrupamento mais expressivo, totalizando 29 ocorrências, o que representa aproximadamente 41,4% do universo amostral. Em seguida, a “Sociedade Civil” comparece com 24 registros (34,3%), indicando que o debate é majoritariamente conduzido por esses dois eixos, que somados perfazem mais de três quartos das contribuições. Os demais segmentos apresentam participação reduzida em termos absolutos: a categoria “Outros” abrange 9 participantes, o “Poder Público” conta com 5 representantes e a “Academia” registra a menor frequência, com apenas 3 entradas. Essa configuração aponta para uma

dinâmica onde o setor privado e a sociedade civil responderam pela maioria das contribuições nesta amostra específica.

Gráfico 1: Distribuição de Participantes por Vínculo Institucional

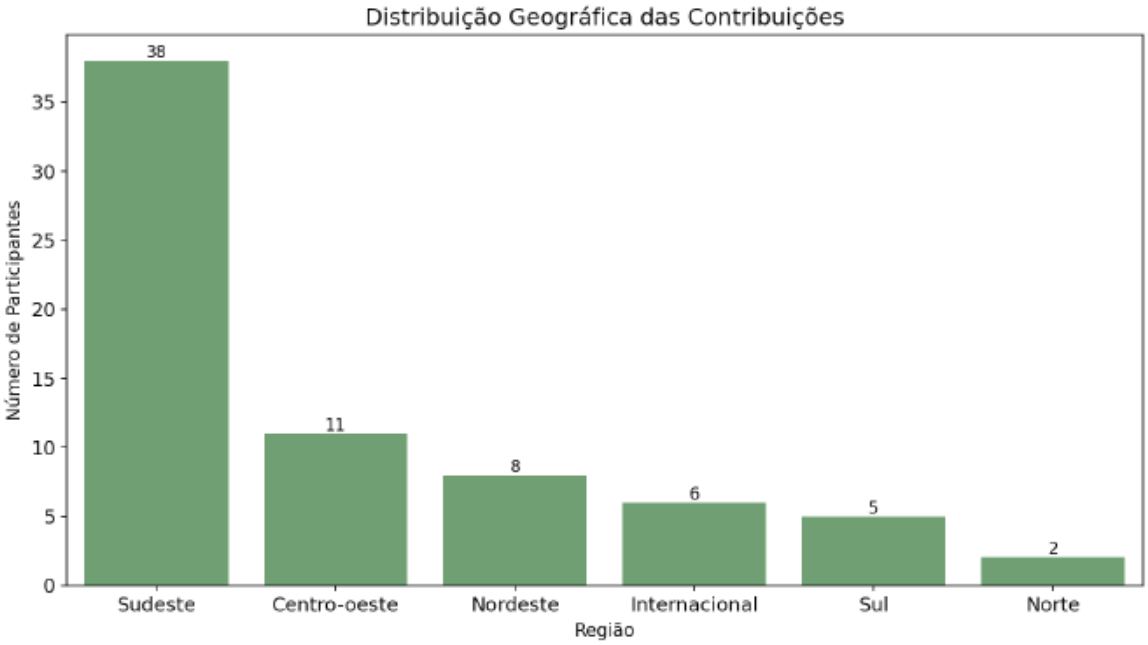


Fonte: produção própria

Análise da distribuição geográfica

A espacialização dos dados, após o processo de normalização que agrupou as entradas “EUA”, “USA” e “UK” sob a categoria “Internacional”, demonstra uma concentração territorial significativa. A região Sudeste lidera o volume de contribuições com 38 participantes, equivalendo a 54,3% do total, mais do que a soma de todas as outras regiões combinadas. O Centro-Oeste figura como a segunda região mais representativa, com 11 registros, seguido pelo Nordeste com 8. A categoria “Internacional” aglutina 6 participantes, superando as regiões Sul (5) e Norte (2). A disparidade regional observada sugere uma centralização das atividades ou do interesse pelo tema no eixo Sudeste, enquanto as regiões Norte e Sul apresentam as menores frequências relativas no conjunto de dados analisado.

Gráfico 2: Distribuição Geográfica das Contribuições



Fonte: produção própria

A interseção entre as variáveis institucional e geográfica permite detalhar como os diferentes setores se distribuem territorialmente, evidenciando padrões de concentração específicos. A matriz de distribuição ilustra que a predominância do Sudeste é impulsionada principalmente pelo “Setor Privado”, que concentra 20 de seus 29 representantes nessa região. Esse dado indica que 69% das empresas participantes estão sediadas no Sudeste. Em contraste, a “Sociedade Civil” apresenta uma dispersão geográfica mais ampla, embora ainda com forte presença no Sudeste (9), também mantém representatividade no Centro-Oeste (5), Nordeste (4) e Sul (4). Outro ponto de destaque é a distribuição dos participantes internacionais: dos 6 registros categorizados como “Internacional”, 5 pertencem ao “Setor Privado” e 1 à “Sociedade Civil”, denotando que a participação externa é quase exclusivamente de natureza empresarial. O “Poder Público” mostra uma distribuição fragmentada com baixa frequência absoluta em qualquer região específica, tendo 2 representantes no Centro-Oeste e 1 nas regiões Norte, Sudeste e Sul, respectivamente. A “Academia”, com seu número reduzido de entradas, restringe-se ao Sudeste (2) e Nordeste (1). A categoria “Outros” alinha-se à tendência geral de concentração, com dois terços de seus integrantes (6 de 9) localizados no Sudeste.

Gráfico 3: Matriz de Distribuição - Instituição vs. Região

Fonte: produção própria

Esta análise cruzada confirma a hipótese de que a centralidade do Sudeste é fortemente correlacionada com a localização das entidades do setor privado, enquanto a sociedade civil demonstra uma capilaridade territorial comparativamente maior. O mapa de calor em escala global reorganiza os dados para evidenciar a participação doméstica e a internacional. A coloração utiliza uma escala logarítmica para permitir a visualização simultânea de magnitudes discrepantes.

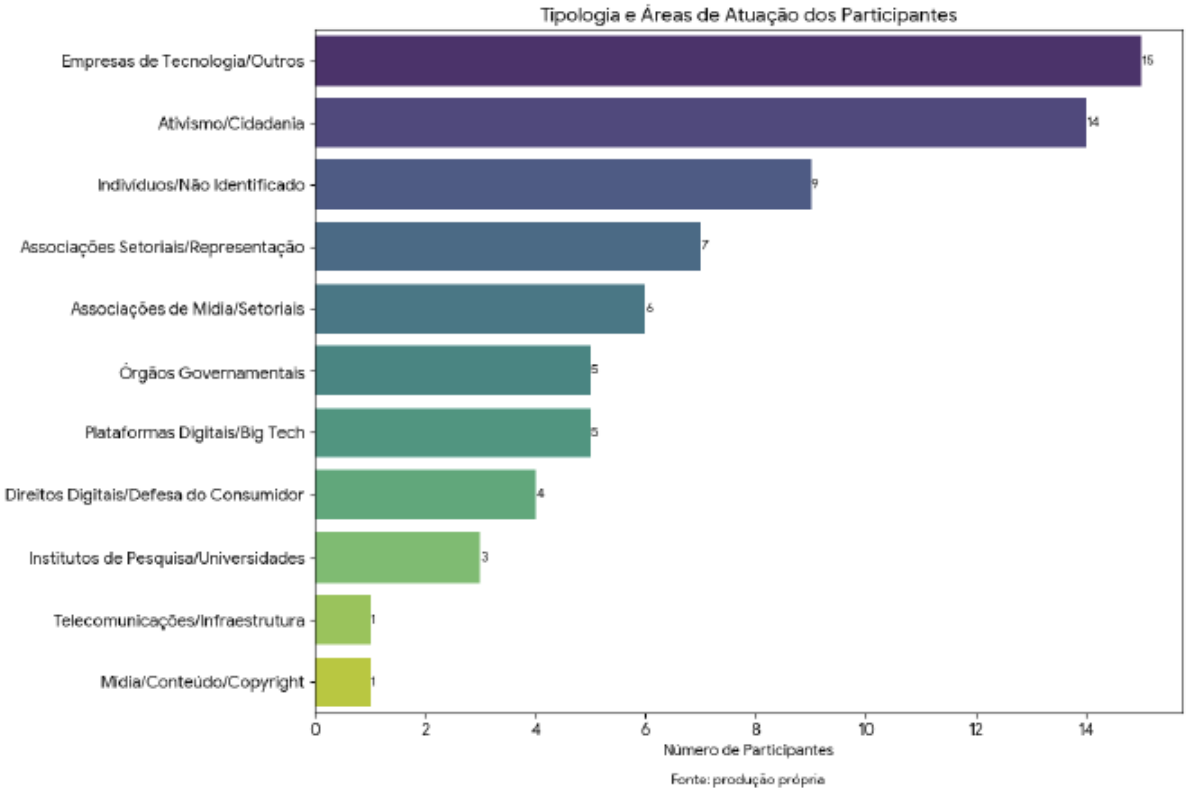
Gráfico 4: Distribuição Espacial das Contribuições (Global)

A agregação dos dados por nacionalidade revela que o Brasil responde por 91,4% de toda a amostra (64 de 70 participantes), consolidando a natureza essencialmente nacional do processo consultivo. Em contrapartida, os Estados Unidos (5 participantes) e o Reino Unido (1 participante) aparecem como atores periféricos, indicando que a participação internacional foi minoritária (8,6% do total) e restrita a atores específicos do hemisfério norte, interessados devido à sua atuação no Brasil. Não houve contribuições de outros países da América Latina, o que pode refletir o escopo nacional da consulta. A visualização confirma que, a despeito da abertura digital que teoricamente permitiria uma participação global difusa, o engajamento real permaneceu circunscrito às fronteiras nacionais e a participantes internacionais restritos.

Análise de tipologia e áreas de atuação

A dissecção qualitativa dos grupos participantes permite identificar subcategorias funcionais que revelam a complexidade dos interesses representados. Para além da divisão institucional primária, observa-se uma fragmentação temática que organiza os atores em clusters de atuação específicos.

Gráfico 5: Tipologia Detalhada dos Participantes



1. O ecossistema do Setor Privado

Dentro do segmento empresarial, a análise semântica das identificações revela quatro vetores distintos:

- **Grandes empresas de tecnologia:** Representado por corporações globais que operam a camada de aplicação e serviços da internet. A presença de entidades como Google, Meta, Epic Games, Match Group (Tinder) e Roku atua em áreas afetadas pela regulamentação de moderação de conteúdo, concorrência digital e responsabilidade de intermediários.

- **Associações setoriais e de representação:** Este é um subgrupo robusto que atua na defesa de interesses coletivos da indústria. Entidades como Zetta, ABES (Software), Brasscom (TIC) e AMOBITEC (Mobilidade) sugerem uma mobilização organizada para influenciar políticas públicas que afetam o ambiente de negócios digitais transversalmente.

- **Empresas de tecnologia e Serviços Específicos:** Um cluster heterogêneo que inclui desde empresas de segurança digital (Kaspersky) e identidade digital (Unico, Yoti) até marketplaces e desenvolvedoras de software (Microsoft, Roblox).

- **Telecomunicações e infraestrutura:** A participação direta de operadoras (*Claro*) sinaliza a presença dos detentores da infraestrutura física de rede, cujos interesses frequentemente divergem dos provedores de aplicação (OTTs).

- **Mídia e conteúdo:** Representado pela *Motion Picture Association - Brasil*, focada na proteção de propriedade intelectual e direitos autorais.

2. As facetas da sociedade civil

As organizações da sociedade civil apresentaram posicionamentos diversificados em pautas de advocacia distintas:

- **Direitos digitais e defesa do consumidor:** Organizações especializadas como *Idec*, *Coalizão Direitos na Rede*, *DiraCom* e *Instituto Alana* (focado na infância) com atuação consolidada na defesa de direitos digitais, priorizando privacidade, liberdade de expressão e proteção de vulneráveis.

- **Associações civis e setoriais:** Inclui associações que representam setores regulados, como a radiodifusão (*ABERT*) e o setor bancário (*Febraban*), além de pautas sociais amplas (*Family Talks*).

- **Ativismo e cidadania:** Contribuições de cidadãos e coletivos para o debate. A presença da *Electronic Frontier Foundation (EFF)* neste grupo adiciona um peso internacional à defesa das liberdades civis digitais.

3. Atores institucionais e acadêmicos

- **Academia:** A participação é qualificada por centros de excelência como o *CTS-FGV Direito Rio*, que aportam embasamento teórico e pesquisa jurídica ao debate regulatório.

- **Poder Público:** A representação estatal é pulverizada, incluindo contribuições de indivíduos vinculados a órgãos públicos e manifestações institucionais como a do *Ministério Público Federal (Comissão de TIC)*, indicando uma preocupação com a aplicabilidade legal e a fiscalização.

- **Outros:** Este grupo residual contém entidades de relevância técnica, como o *CGI.br* (Comitê Gestor da Internet no Brasil) e a *ABINEE* (Indústria Elétrica e Eletrônica)/

Essa estratificação demonstra que a consulta pública mobilizou não apenas empresas e cidadãos, mas uma diversidade de perspectivas setoriais representadas.

3. ANÁLISE DOS EIXOS TEMÁTICOS

3.1 EIXO 1: Diagnóstico e Atribuição de Responsabilidade (DIAG)

3.1.1 Visão geral e definição do eixo

Este eixo temático sintetiza os argumentos sobre a alocação de deveres e a definição dos pressupostos da intervenção regulatória, oscilando entre a reafirmação da autoridade parental como barreira primária de controle e o reconhecimento técnico da obsolescência da autodeclaração como método de segurança. Contribuintes do setor privado apresentaram argumentos em defesa da primazia familiar, sustentando que o papel das empresas é fornecer ferramentas de gestão, não substituir o juízo dos responsáveis, enquanto organizações da sociedade civil apontam a inviabilidade prática do monitoramento parental integral. Simultaneamente, identifica-se um segmento de argumentos céticos que alertam para os riscos colaterais da regulação, como o deslocamento de usuários para jurisdições não supervisionadas e o aumento da vulnerabilidade de dados, o que fundamenta a defesa jurídica das empresas pelo princípio da responsabilidade solidária constitucional e pela adoção de um padrão de devida diligência, onde a aplicação de melhores esforços técnicos deve eximir as empresas de punição objetiva em casos de evasão ou fraude pelo usuário.

3.1.2 Frequência e relevância dos temas

A distribuição de frequência os temas na categoria Diagnóstico e Responsabilidade (DIAG) indica que a discussão sobre a alocação de deveres se sobrepõe à análise técnica do problema, com a maior concentração de unidades (16) no código *DIAG_PRIMAZIA_FAMILIAR*, o qual situa a autoridade parental como o mecanismo primário de controle de acesso, em detrimento da mediação tecnológica exclusiva. Em segundo plano, o código *DIAG_CETICISMO_DANOS* (11) agrupa argumentos que questionam a eficácia da intervenção regulatória frente a riscos colaterais como o deslocamento de usuários para jurisdições externas e a coleta excessiva de dados. A fundamentação jurídica da defesa corporativa compõe um bloco significativo quando somados os códigos *DIAG_RESP_SOLIDARIA* (8) e *DIAG_DEVIDA_DILIGENCIA* (5), totalizando 13 unidades que articulam a proteção como dever constitucional compartilhado e estabelecem o padrão de melhores esforços como limite para a imputabilidade das empresas. Por fim, o

código *DIAG_FALHA_AUTO*(7) registra o reconhecimento transversal da insuficiência dos métodos declaratórios vigentes, consolidando o diagnóstico de que o modelo atual de autenticação de usuário carece de eficácia verificável.

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
DIAG_PRIMAZIA_FAMILIAR	16	Argumentos que reafirmam o papel da supervisão parental como elemento central da proteção. Enfatizam que a tecnologia de verificação é complementar e que a educação digital das famílias constitui a barreira primária.
DIAG_CETICISMO_DANOS	11	Questionamentos sobre a eficácia da verificação obrigatória, com alertas sobre riscos de exclusão digital, migração de usuários para ambientes não regulados ou efeitos colaterais indesejados da intervenção.
DIAG_RESP_SOLIDARIA	8	Invocação do Art. 227 da Constituição Federal e do ECA para sustentar que a proteção é dever compartilhado entre Estado, família e sociedade. Sustenta que a responsabilização não deve recair exclusivamente sobre as plataformas.
DIAG_FALHA_AUTO	7	Diagnóstico de que a autodeclaração de idade é estruturalmente insuficiente. Argumentos de que o modelo de "autenticação de usuário" deve ser substituído por mecanismos de verificação de idade mais robustos.
DIAG_DEVIDA_DILIGENCIA	5	Argumentos sobre limites da responsabilidade empresarial: se a plataforma adotou medidas razoáveis (*best efforts*), questionam a responsabilização objetiva em casos de evasão do sistema pelo usuário ou por terceiros.
TOTAL	**47**	

3.1.3 Principais argumentos

A. O consenso da falha na autodeclaração

Há um consenso de que os métodos atuais de autodeclaração, por si só, são insuficientes para casos de alto risco. O FNPETI é incisivo ao declarar a “manifesta ineficácia” da autodeclaração, argumentando que ela “transfere a responsabilidade integralmente ao usuário e exime fornecedores de sua responsabilidade legal”. O Instituto Alana reforça que banir a autodeclaração força as empresas a “abandonarem sua zona de conforto… empurrando as empresas para um cenário onde a proteção… não são opcionais” e define o momento como uma “transição do paradigma da ‘autenticação do usuário’ para a ‘autenticação da idade’

Contribuintes do setor privado (representada pela ABA e Samsung) admitem a falha, mas para justificar o ceticismo sobre *qualquer* solução: “A declaração de idade já foi criticada por sua falta de confiabilidade… [mas] a estimativa de idade também pode ser burlada”. Eles usam a falha da autodeclaração para pedir cautela na imposição de novas tecnologias que também podem ser burladas.

B. A tese da primazia familiar

Contribuintes do setor privado apresentaram argumentos que posicionam a responsabilidade final junto aos pais, enquadrando a tecnologia como ferramenta de apoio à autoridade parental. A Meta argumentou que mecanismos de aprovação parental para downloads capacitam as famílias, defendendo arquiteturas de controle baseadas em permissão, e não em verificação intrusiva: “a aprovação parental para downloads de aplicativos é o fator decisivo… capacitando as famílias e, ao mesmo tempo, mantendo os padrões regulatórios”. Para a Meta, a solução ideal é aquela que reforça a hierarquia doméstica: “Mecanismos centralizados… dão aos pais mais supervisão e controle”.

Esta visão é amplamente corroborada pelas associações industriais, que utilizam a primazia familiar para limitar a responsabilidade corporativa. A Claro S.A. e a Samsung repetem, *ipsis litteris*, que o dever de vigilância “decorre diretamente do papel de guarda e vigilância do ECA e não pode ser transferido ao setor privado”. A Câmara Brasileira da Economia Digital expande esse argumento para a esfera da autonomia cultural, alertando que “O que uma família considera adequado… pode ser visto de maneira diferente por outra, e não cabe às empresas substituir esse juízo”.

No entanto, a PROTESTE contesta a viabilidade prática dessa primazia em um cenário de complexidade tecnológica. Embora reconheça o papel da família, argumenta que a “aferição de idade reduz desigualdades e limitações que tornam impraticável exigir que pais… monitorem integralmente ambientes digitais complexos”. Para os representantes da sociedade civil, insistir apenas na responsabilidade parental é ignorar a assimetria de poder entre pais exaustos e algoritmos viciantes

C. A tese da responsabilidade solidária

Diversos contribuintes invocaram o conceito de responsabilidade solidária para fundamentar suas posições sobre a distribuição de obrigações entre os agentes envolvidos na proteção de crianças e adolescentes no ambiente digital.

Contribuintes do setor de telecomunicações e hardware, como Claro S.A., BRASSCOM e Federação do Comércio de SP, argumentaram que a proteção constitui dever compartilhado entre "Estado, famílias, sociedade civil e setor privado", sustentando que "a responsabilização não deve recair exclusivamente sobre as empresas". Esses contribuintes fundamentaram suas posições no artigo 227 da Constituição Federal e no próprio ECA Digital.

A Meta aderiu a essa perspectiva, citando o Artigo 15 do ECA Digital por "estabelecer responsabilidade compartilhada e solidária", e defendendo uma abordagem de "ecossistema completo" na qual diferentes atores assumem parcelas distintas da responsabilidade.

A Federação do Comércio de SP argumentou que essa responsabilidade compartilhada implica que o Estado deve prover "políticas públicas de educação digital" como componente da estratégia de proteção.

Por outro lado, contribuintes da sociedade civil, como a PROTESTE, questionaram a operacionalização prática desse conceito, argumentando que a "aferição de idade reduz desigualdades e limitações que tornam impraticável exigir que pais monitorem integralmente ambientes digitais complexos". Para esses contribuintes, a invocação da responsabilidade familiar não pode servir para eximir empresas de obrigações proporcionais ao risco que seus serviços apresentam.

A tensão identificada reside na definição do conteúdo concreto da responsabilidade de cada ator: enquanto parte dos contribuintes do setor privado enfatizou o papel da família e do Estado como condição para delimitar suas próprias obrigações, contribuintes da sociedade civil sustentaram que as empresas, por criarem e controlarem os ambientes de risco, devem assumir obrigações proporcionais independentemente da atuação dos demais agentes.

D. A estratégia da prevenção

A definição do dever de prevenção é disputada para estabelecer até onde vai a obrigação da plataforma. A Samsung e a Federação do Comércio argumentam que a responsabilidade das plataformas vai até o limite da *"medida razoável"*. Se a empresa adotou mecanismos proporcionais, ela não pode ser culpada se *"o menor não se faça passar pelo referido responsável legal"* (como com o uso de identidade falsa ou dispositivo dos pais). A BRASSCOM reforça que *"é necessário reconhecer os limites da atuação das empresas… visto que mesmo com medidas técnicas adequadas, é possível que ocorram usos irregulares"*. O conceito chave é *"best efforts"*(melhores esforços): a empresa garante o meio (ferramenta de verificação), mas não pode garantir o resultado (bloqueio total) se houver dolo do usuário ou negligência dos pais.

A Claro S.A. introduz o cenário de fraude doméstica para limitar sua diligência: "caso um dos responsáveis legais disponibilize seu aparelho… a verificação de idade se revelaria ineficaz". O argumento é que a devida diligência técnica da empresa cessa onde começa a negligência parental.

E. O ceticismo sobre os danos

Há, ainda, argumentos que questionam a eficácia ou os pressupostos da intervenção estatal para aferição de idade e sua capacidade de mitigar riscos. A Associação Brasileira de Anunciantes (ABA) introduz o conceito de risco deslocado, alertando que a verificação obrigatória pode *"incentivar os usuários a migrarem para jurisdições menos restritivas… expondo-os… a riscos maiores"*. Para a ABA, a regulação local cria *"paraísos digitais"* inseguros.

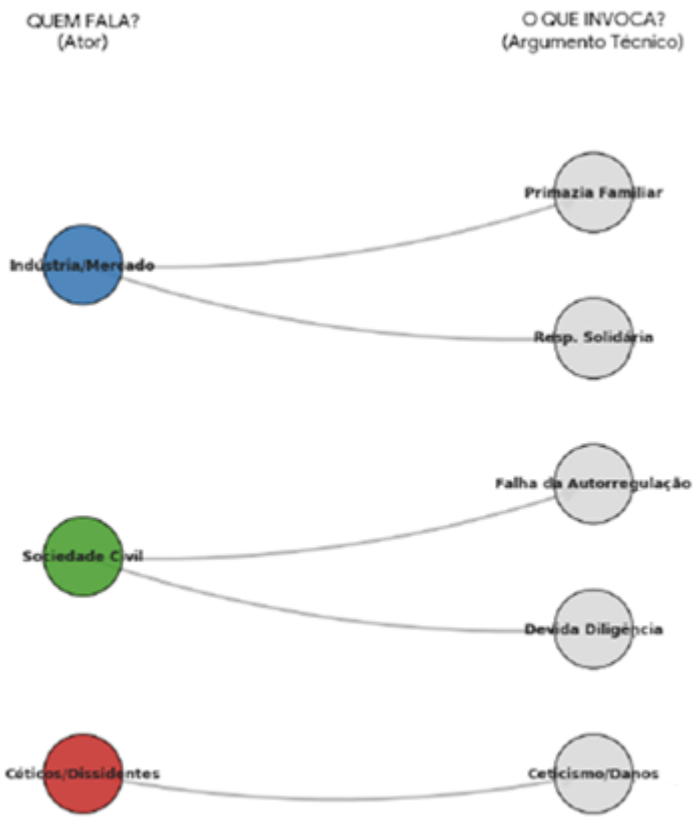
Um contribuinte da sociedade civil apresentou questionamentos sobre os pressupostos da regulação, argumentando que a proteção infantil não deveria servir de fundamento para medidas que poderiam resultar em restrições desproporcionais ao acesso à informação. O ator argumenta que *"a proteção das crianças é apenas uma ferramenta, a 'imagem' do movimento, e não seu verdadeiro objetivo"*, sugerindo que a regulação visa o controle social e não a segurança. Ele alerta para um efeito rebote: *"manter as crianças como crianças levará à ascensão de adultos que se comportam como crianças"*, criticando a infantilização da sociedade.

A Electronic Frontier Foundation (EFF) traz um ceticismo técnico, argumentando que a coleta massiva de dados para verificação resulta na *"ampliação da superfície de ataque e maior vulnerabilidade a vazamento"*. O ceticismo aqui não é moral, mas de engenharia de segurança: criar bases de dados de crianças é criar vetores de ataque.

3.1.4 Terminologia e conceitos-chave

A Figura 1 representa uma visualização qualitativa que mapeia a estrutura argumentativa de cada grupo de contribuintes, identificando os fundamentos apresentados para sustentar suas posições.

Figura 1: Fluxo de argumentação dos atores



Fonte: produção própria

1. **Azul - Indústria:** Argumentos que enfatizam a primazia familiar e os limites da responsabilidade empresarial.

2. **Verde - Sociedade Civil:** Argumentos que partem do diagnóstico de insuficiência da autorregulação para defender obrigações de resultado.

3. **Vermelha - Contribuintes com ressalvas: A**rgumentos que questionam premissas da intervenção regulatória.

Esta representação visual demonstra como os atores estão operando em **paradigmas paralelos** que raramente se cruzam.

Quadro Comparativo: Argumentos de Legitimação por Setor (LEGIT)

GRUPO DE CONTRIBUINTES	ÊNFASE NA ATRIBUIÇÃO DE RESPONSABILIDADE	ARGUMENTO CENTRAL	IMPLICAÇÃO PARA A REGULAMENTAÇÃO
Setor Privado	Família como agente primário; Plataforma como facilitadora	A supervisão do acesso digital é atribuição dos pais, cabendo às plataformas fornecer ferramentas de apoio. A empresa não deve substituir o juízo familiar sobre o que é adequado.	Regulamentação deve priorizar instrumentos de controle parental e evitar responsabilização objetiva das plataformas por falhas de supervisão familiar.
Sociedade Civil e Organizações de Defesa de Direitos	Plataforma como agente primário; Estado como regulador	A complexidade dos ambientes digitais e a assimetria de informação tornam a supervisão parental insuficiente. O risco é inerente ao design dos serviços, cabendo às empresas adotar medidas proativas de proteção (*safety by design*).	Regulamentação deve estabelecer obrigações de resultado para as plataformas, com devida diligência independente da atuação dos pais.
Contribuintes com ressalvas sobre eficácia	Mercado global como fator condicionante	Barreiras rígidas podem deslocar usuários para ambientes não regulados, reduzindo a eficácia da proteção pretendida. Alerta para riscos de efeitos colaterais da intervenção.	Regulamentação deve considerar dinâmicas de migração de usuários e adotar abordagem proporcional que não incentive a evasão para jurisdições sem proteção.

GRUPO DE CONTRIBUINTES	ÊNFASE NA ATRIBUIÇÃO DE RESPONSABILIDADE	ARGUMENTO CENTRAL	IMPLICAÇÃO PARA A REGULAMENTAÇÃO
Contribuintes com ressalvas sobre legitimidade	Questionamento das premissas da intervenção	Questionamentos sobre a base empírica dos danos alegados e sobre os limites da intervenção estatal em matéria de acesso à informação.	Regulamentação deve fundamentar-se em evidências e respeitar limites constitucionais relativos à liberdade de expressão e acesso à informação.

3.2 Eixo 2: Escopo e Definição do Objeto Regulado (ESCO)

3.2.1 Visão geral e definição do eixo

A análise do eixo de “Escopo e Modulação Setorial” revela uma estrutura argumentativa fundamentada na rejeição de modelos de aplicação universal da lei em favor de uma lógica de proporcionalidade e escalonamento por matrizes de risco. Enquanto há convergência entre os atores sobre a necessidade de isenções para setores já regulados ou com finalidades utilitárias específicas (como serviços financeiros , conteúdo editorial e redes profissionais), a definição dos critérios de “Alto Risco” apresenta divergências estruturais: organizações da sociedade civil e contribuintes da academia associaram o risco aos modelos de negócio e algoritmos de recomendação, enquanto contribuintes do setor privado propuseram limitar o escopo. Transversalmente, a discussão sobre a responsabilidade opõe a demanda por focar as obrigações nos “gatekeepers” para preservar a competitividade de pequenos agentes aos alertas sobre os riscos de centralização de dados e vigilância inerentes à concentração da identificação em poucos atores sistêmicos

3.2.2 Frequência e relevância dos temas

A distribuição de frequência dos temas que aparecem neste eixo evidencia uma concentração preponderante na definição estrutural da aplicabilidade normativa, com metade das unidades de conteúdo (41 de 82) dedicadas aos códigos *ESCO_MATRIZ_RISCO* (22) e *ESCO_DEF_RISCO* (19), o que indica que a discussão central reside no estabelecimento de critérios de gradação e na tipificação do que constitui risco, em detrimento de abordagens uniformes. Em um segundo nível de relevância, observam-se demandas específicas de direcionamento regulatório, com 11 unidades focadas na responsabilização das grandes plataformas sistêmicas

(*ESCO_GATEKEEPERS*) e 10 unidades voltadas ao bloqueio estrito de conteúdos de alto dano (*ESCO_CONTEUDO_PROIBIDO*). O segmento restante, compondo aproximadamente um quarto do *corpus* (20 unidades), agrupa as reivindicações de exclusão setorial, distribuídas entre o setor financeiro (*ESCO_ISENCAO_FINANCEIRO*, 8), jornalístico (*ESCO_ISENCAO_EDITORIAL*, 7) e redes profissionais (*ESCO_ISENCAO_PROFISSIONAL*, 5), fundamentando a defesa de que ambientes já regulados ou de finalidade laboral devem permanecer fora do escopo de novas exigências de verificação etária.

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
ESCO_MATRIZ_RISCO	22	Discussões sobre a gradação da verificação baseada no risco. Argumentos de que as exigências devem ser proporcionais ao nível de risco do serviço (alto risco vs. baixo risco).
ESCO_DEF_RISCO	19	Discussões sobre a definição do que constitui "risco" ou "dano". Distinções entre conteúdo nocivo e conteúdo ilegal.
ESCO_GATEKEEPERS	11	Discussões sobre o foco regulatório nas grandes plataformas sistêmicas. Argumentos sobre se as obrigações devem ser mais rigorosas para plataformas com maior poder de mercado.
ESCO_CONTEUDO_PROIBIDO	10	Discussões sobre regras específicas para conteúdo adulto, jogos de azar e conteúdos legalmente restritos a maiores de 18 anos, onde contribuintes propuseram bloqueio de acesso a menores.
ESCO_ISENCAO_FINANCEIRO	8	Argumentos para tratamento diferenciado de setores financeiros (bancos, fintechs) que já possuem regulação própria de verificação de identidade (KYC bancário).
ESCO_ISENCAO_EDITORIAL	7	Argumentos sobre liberdade de imprensa e tratamento diferenciado para veículos de mídia e jornalismo.
ESCO_ISENCAO_PROFISSIONAL	5	Argumentos para tratamento diferenciado de redes profissionais e ferramentas de trabalho corporativo.
TOTAL	**82**	

3.2.3 Principais Argumentos

A. Foco em conteúdo proibido

As respostas demonstram uma disputa sobre a extensão do mandato de aferição de idade: se restrito ao ilegal ou expandido ao nocivo. A Câmara Brasileira da Economia Digital defende uma aplicação minimalista, focada na tipificação criminal, onde “recomenda-se que a obrigatoriedade de verificação de idade seja reservada a conteúdos manifestamente de alto risco - como pornografia e materiais explicitamente proibidos por lei - nos quais o potencial de dano é inequívoco”. O Google Brasil reforça essa perspectiva, enquadrando a verificação como uma ferramenta de adequação de produto para adultos, afirmando que “onde os serviços são destinados a usuários maiores de 18 anos, o restringir o acesso com base na idade é uma mitigação importante para reduzir o risco de que crianças ou adolescentes tenham acesso a serviços que não foram projetados para eles”.

A AMOBITEC sugere uma aplicação cirúrgica da verificação, limitada a transações específicas dentro de serviços mais amplos, argumentando que “A implementação de controles específicos deve ser direcionada apenas para funcionalidades restritas (tais como o ato de compra de produtos para maiores de 18 anos), permitindo que o restante do serviço permaneça acessível sem barreiras desnecessárias”.

Em oposição, o Instituto Alana contesta a suficiência dessa abordagem restrita, defendendo que a proteção deve abranger riscos não criminais, mas desenvolvimentais, argumentando que “é necessário restringir o acesso … não para limitar sua participação … mas sim para resguardá-los dos riscos desproporcionais … Até mesmo países como a Itália … entendem ser necessário bloquear o acesso desses indivíduos a conteúdos prejudiciais, como o pornográfico”. A Family Talks aponta a impossibilidade prática de separar conteúdos em redes abertas, notando que “estão disponíveis na rede, misturados sem nenhum crivo, tanto conteúdos positivos quanto nocivos … a expansão da internet resultou na disseminação de todo tipo de conteúdo, acessível a qualquer público”, o que exigiria uma verificação mais ampla do que apenas em sites “proibidos”. A Meta, por sua vez, tenta posicionar a tecnologia de IA como mediadora dessa complexidade,

afirmando: “Usamos essa tecnologia para impedir que adolescentes acessem recursos destinados a adultos … e garantir que o conteúdo que os adolescentes veem seja adequado à idade”.

B. Definição ampliada de risco

A definição do que constitui “risco” é disputada entre uma visão acadêmica estrutural e uma visão corporativa funcional. O Comitê Gestor da Internet no Brasil (CGI.br) fundamenta sua definição na literatura de Sonia Livingstone, estabelecendo que “A tipologia dos “4Cs” … corrobora a necessidade de se considerar diferentes contextos … sendo eles: Conteúdo …, Contato …, Conduta … e Contrato/Commerce”. Esta base teórica é sugerida como diretriz fiscalizatória pelo Ministério Público Federal (MPF), que qualifica o risco pela ausência de mediação, afirmando que “Um serviço deve ser classificado como de maior risco quando envolve comunicação não moderada e aberta entre adultos e crianças (risco de aliciamento), exposição a conteúdo ilegal … e a possibilidade de danos financeiros”.

A Coalizão Direitos na Rede e o Instituto Alana aprofundam a análise para além do conteúdo, focando na arquitetura de persuasão. A Coalizão argumenta que o risco reside no modelo de negócio, onde “os seus serviços são desenhados de modo a estimular maior tempo de tela e engajamento … as crianças e adolescentes ficam expostas a riscos de recomendação de conteúdos nocivos, aliciamento, publicidade inapropriada”, enquanto o Alana especifica que o perigo emana de “Mecanismos que induzem uso compulsivo … Exemplos de recursos arriscados são algoritmos de personalização, feed infinito e modelos de vídeos curtos”. A uma contribuinte acadêmica corrobora essa visão, adicionando a autonomia como variável crítica: “Grau de interação social e exposição a terceiros – especialmente quando há comunicação direta com desconhecidos … Nível de autonomia exigido para o uso do serviço – quanto maior a autonomia … maior o risco associado”.

Em contrapartida, o setor privado busca atenuar essa classificação através da existência de ferramentas de controle. O Match Group (Tinder) argumenta que a arquitetura fechada de mensagens reduz a periculosidade, declarando que “*services like Match Group’s dating apps, where interactions occur primarily through private messages, pose a more controlled risk … Another important criterion to consider is*

content sensitivity". Similarmente, a Roblox defende que a presença de mecanismos de segurança deve ser um fator de desclassificação de risco, sustentando que "A existência de proteções por padrão … devem ser consideradas como fatores atenuantes para a classificação dos serviços de acordo com o risco". Percebe-se, portanto, uma divergência ontológica: para a sociedade civil, o risco é intrínseco ao design de engajamento; para as plataformas, o risco é mitigável pelas ferramentas de gestão.

C. Proposta de matriz de risco

Os dados mostram uma tensão fundamental entre a universalidade da proteção e a viabilidade econômica do ecossistema digital. A Câmara Brasileira da Economia Digital (camara-e.net) estabelece a premissa de que a heterogeneidade dos serviços demanda uma aplicação regulatória assimétrica, argumentando que "Serviços distintos demandam controles distintos, e não é adequado impor a mesma intensidade de verificação de idade a plataformas com finalidades, formatos de interação e perfis de risco evidentemente diversos". Esta posição introduz o argumento da proporcionalidade como mecanismo de sobrevivência econômica, uma vez que a mesma entidade alerta que "Classificações desproporcionais, baseadas apenas na existência de uma funcionalidade isolada, podem gerar barreiras indevidas, prejudicar a inovação e limitar o acesso a conteúdos adequados para diferentes faixas etárias".

A concordância com essa modulação é expressa por diversos participantes do setor privado, como a Microsoft, que desloca o foco da tecnologia para a natureza do dano, sustentando que "serviços online que apresentem baixo risco de gerar os danos enumerados no Artigo 6º … não devem ser obrigados a implementar verificação de idade, mas sim utilizar métodos de garantia de idade proporcionais ao risco". No entanto, a operacionalização dessa matriz revela complexidades técnicas, conforme aponta o Instituto Teckids, ao observar que a taxonomia de risco não é linear, dado que "Diferentes plataformas apresentam riscos distintos seja pela natureza do conteúdo, pela interação social, pela sensibilidade de tratamento dos dados, nível de exposição", sugerindo que a simplificação binária (alto/baixo risco) pode ser insuficiente.

A Fecomercio-SP expande o debate para a esfera da segurança jurídica, defendendo que uma matriz de risco funcionaria como um garantidor de previsibilidade para o mercado, afirmando ser "fundamental que os critérios de classificação sejam claros, proporcionais e previsíveis, garantindo segurança jurídica e permitindo que as organizações planejem adequadamente seus mecanismos de conformidade". Em uma perspectiva pragmática de implementação, a AMOBITEC propõe que a verificação seja circunstancial e não estrutural para serviços de menor risco, sugerindo que "poder-se-ia considerar que, em plataformas de menor risco, a aferição de idade ocorra no momento da compra". O Mercado Livre reforça essa lógica de isenção para interações de baixo risco, argumentando que "Plataformas que não têm como atividade principal a interação social ou a disponibilização de conteúdo voltado para o entretenimento, não devem ser equiparadas às redes sociais".

Assim, percebe-se uma rejeição unânime do setor produtivo à abordagem "tamanho único", fundamentada tanto na incapacidade técnica de pequenos atores quanto na inadequação conceitual de tratar ferramentas utilitárias como vetores de risco sistêmico.

D. Foco nos *gatekeepers*

Há uma patente preocupação com a assimetria de poder e a capacidade de implementação. A Kaspersky Lab introduz o argumento de que a regulação uniforme pode paradoxalmente reduzir a segurança ao eliminar a diversidade de mercado, alertando que "Mandatos excessivamente prescritivos ou de alto custo podem criar barreiras, especialmente para startups e pequenos desenvolvedores, reduzindo diversidade e competição no mercado digital". O CGI.br alinha-se a essa preocupação econômica, recomendando "que a regulamentação preveja explicitamente tais exceções, assegurando inovação, inclusão digital, para pequenos provedores", sugerindo que o ônus regulatório deve ser proporcional ao porte econômico.

O Centro de Tecnologia e Sociedade (CTS-FGV) propõe uma hierarquização da responsabilidade baseada na posição na cadeia de valor, argumentando que "existe uma expectativa maior de diligência devida para players com poder econômico na cadeia de valor que leva ao contato com os usuários na ponta, como é frequentemente

o caso de provedores de lojas de aplicações". Contudo, essa centralização da responsabilidade nos "*gatekeepers*" é vista com ceticismo por outros atores sob a ótica da privacidade. Um contribuinte da academia adverte que delegar essa função às grandes plataformas agrava o monitoramento, pois "As *big techs* como Meta e Google certamente ofereceram mecanismos próprios … é necessária a fiscalização de tais mecanismos para evitar que eles … sejam um vetor de coletar ainda mais dados pessoais".

A Unico - IDTech expande essa crítica para o risco democrático de um ponto único de falha ou controle, argumentando que "A centralização excessiva pode transformar a identidade digital e aferição de idade em instrumento de controle, e não de confiança, tornando o cidadão dependente e rastreável por um único *gatekeeper* estatal". Assim, o debate sobre gatekeepers oscila entre a necessidade econômica de proteger os pequenos competidores e o receio político e social de conceder ainda mais poder de dados aos grandes conglomerados ou ao Estado.

E. Isenção de determinados setores

Com relação ao setor financeiro, observa-se um consenso setorial sobre a redundância regulatória. A Fecomercio-SP argumenta que o setor já opera sob estrita vigilância de identidade, tornando novas camadas de verificação desnecessárias, ao afirmar que "Serviços financeiros, bancos e seguradoras já cumprem rigorosas normas de KYC (Know Your Customer) e BACEN, devendo ser isentos de novas obrigações de verificação". Esta posição é reforçada pela Zetta, que distingue o risco transacional do risco de interação social, defendendo que "O risco deve ser avaliado não apenas pelo conteúdo, mas pelas features de design … Aplicativos de bancos não oferecem risco de conteúdo ou contato perigoso".

A Câmara Brasileira da Economia Digital complementa essa visão ao enfatizar a pontualidade da interação em e-commerce, o que justificaria isenção de verificações de acesso contínuo, argumentando que "Em plataformas cujo risco é pontual - como a compra de itens legalmente restritos - a verificação deve ocorrer de forma precisa e direcionada, preservando o acesso amplo e sem fricção às demais áreas do serviço". A ausência de contrapontos significativos neste código sugere que a natureza utilitária

e já regulada do setor financeiro é amplamente aceita como fora do escopo primário da nova regulação de proteção infantil online.

A distinção entre curadoria profissional e conteúdo gerado pelo usuário (UGC) fundamenta os argumentos de pedido de isenção para serviços e aplicações com controle editorial. Representantes do setor de mídia e entretenimento argumentam que a existência de uma linha editorial atua como um mecanismo de segurança *ex ante*. As unidades de conteúdo indicam que “O conteúdo editorialmente controlado não apresenta os mesmos riscos de algoritmos viciantes ou contato com estranhos”, estabelecendo uma dicotomia clara com as redes sociais. A comparação direta é utilizada para ilustrar a desproporcionalidade, onde se afirma que “A regulação não deve equiparar a Netflix ou um portal de notícias ao TikTok. A dinâmica de risco é oposta”.

Além do aspecto técnico, emerge uma defesa baseada em direitos fundamentais, onde se argumenta que “Jornais e revistas digitais devem ser isentos para garantir o direito à informação e liberdade de imprensa”, sugerindo que barreiras de idade poderiam cercear o acesso cívico. A eficácia dos sistemas atuais de classificação indicativa é evocada como suficiente, com o argumento de que “Plataformas de VOD já seguem a classificação indicativa do Ministério da Justiça; impor nova verificação seria redundante”.

Por fim, há uma preocupação específica com plataformas voltadas para o desenvolvimento profissional. O argumento é que estas possuem dinâmicas de interação distintas e monitoradas pelo próprio contexto “de negócios”. As unidades destacam que “Plataformas focadas exclusivamente em carreira e emprego … não devem ser sujeitas às mesmas regras de redes de entretenimento”.

Há uma ênfase no impacto negativo que barreiras de entrada poderiam ter sobre a demografia de jovens em início de carreira, com a alegação de que “Adolescentes a partir de 14 ou 16 anos usam essas redes para buscar trabalho. A verificação rigorosa pode ser um obstáculo à sua inserção profissional”. A natureza das interações é utilizada para afastar a presunção de risco, argumentando-se que o ambiente possui um “tratamento regulatório diferenciado e mais brando” devido ao

baixo risco de práticas predatórias como *grooming* em ambientes corporativos transparentes.

3.2.4 Terminologia e conceitos-chave

A análise transversal do léxico in vivo nesta categoria revela uma disputa semântica que opõe a gramática da "proporcionalidade" e da "matriz de risco" ao vocabulário da universalidade, frequentemente rejeitado sob o anglicismo "*one-size-fits-all*". Os participantes estruturam seus argumentos mobilizando uma taxonomia técnica que diferencia o "risco sistêmico" do "risco pontual". O termo "*tiers*" (níveis) emerge nativamente como a solução estrutural para essa diferenciação, onde se busca evitar que a regulação crie "barreiras indevidas" ou "custo de conformidade" que inviabilizem a "inovação" de "pequenos desenvolvedores" e do "Fediverso". A terminologia utilizada para descrever o objeto da regulação transita entre o jurídico e o arquitetural: enquanto o setor privado foca em "funcionalidades restritas" e "conteúdo manifestamente de alto risco" (limitado a "pornografia" e "ilegalidade"), a sociedade civil e a academia introduzem o vocabulário do design comportamental, citando "algoritmos viciantes", "feed infinito", "*dark patterns*", "economia da atenção" e "mecanismos de *gacha*" ou "*loot boxes*".

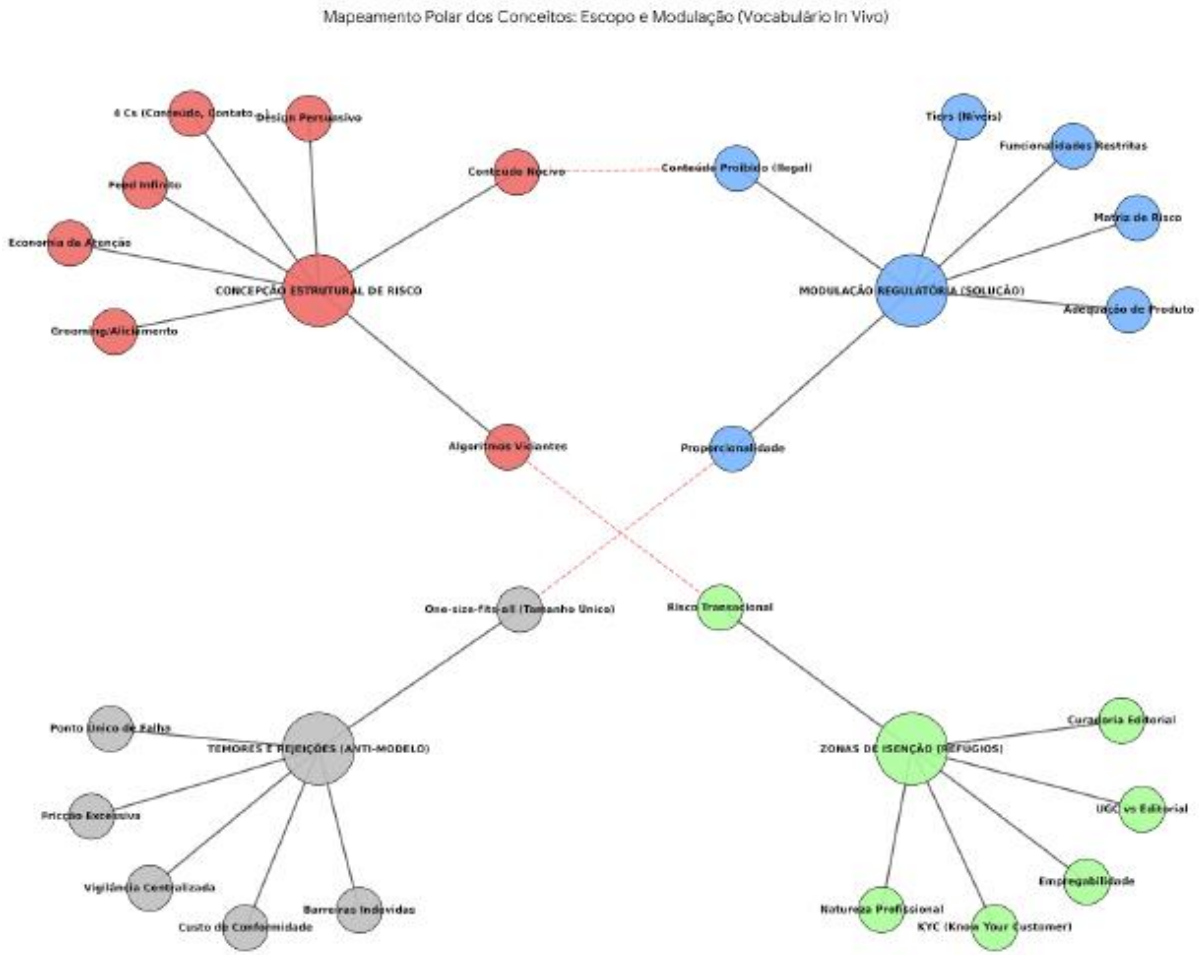
A definição de periculosidade é operada através do conceito dos "4 Cs" ("Conteúdo", "Contato", "Conduta" e "Contrato"), que serve como léxico fundamental para classificar o que constitui um ambiente de "alto risco". O termo "*grooming*" e "*sexting*" aparecem como descritores específicos das ameaças de interação, frequentemente contrastados com ambientes que possuem "curadoria editorial" ou "interação monitorada". No debate sobre a sujeição passiva à norma, o termo "*gatekeepers*" é apropriado nativamente do vocabulário antitruste para designar as grandes empresas de tecnologia posicionadas como os únicos atores com capacidade de "devida diligência" sem gerar "fricção" excessiva. Em oposição, termos como "ponto único de falha" e "rastreável" denotam o medo da vigilância centralizada.

Para justificar exclusões, o léxico se torna utilitário e tecnocrático: o setor financeiro mobiliza a sigla KYC ("*Know Your Customer*") e o termo "risco transacional" para se diferenciar do "risco social" ou "comportamental". O setor de

mídia utiliza a distinção entre UGC ("*User Generated Content*" ou Conteúdo Gerado pelo Usuário) e "conteúdo editorialmente controlado". Já no âmbito profissional, a "empregabilidade" e a "inserção profissional" funcionam como palavras-chave para re-significar o acesso à plataforma não como entretenimento, mas como necessidade econômica, afastando a terminologia de "vício" ou "dano psíquico" associada às redes sociais. A distinção semântica final reside na dicotomia entre "conteúdo nocivo" (que exige moderação) e "conteúdo proibido" (que exige barreira), demonstrando que o debate regulatório envolve também a definição dos termos que delimitam a arquitetura da internet.

A Figura 2 representa o mapeamento polar dos Conceitos, uma representação alternativa que organiza o vocabulário em quatro quadrantes de sentido (Polos) que estruturam o debate.

Figura 2: Posições sobre o Escopo da Regulação



Fonte: produção própria

As linhas tracejadas em vermelho indicam as tensões dialéticas: como a “Proporcionalidade” surge para combater o “*one-size-fits-all*”, e como o conceito de “conteúdo nocivo” (vermelho) desafia a limitação ao “conteúdo proibido” (Azul).

Quadro Comparativo: Posições sobre Escopo e modulação setorial (ESCO)

DIMENSÃO ANALÍTICA	BLOCO 1: SETOR PRIVADO E PLATAFORMAS	BLOCO 2: SOCIEDADE CIVIL E ACADEMIA	BLOCO 3: CONTRIBUINTES COM ÊNFASE EM PRIVACIDADE E SOBERANIA
Definição do risco	**Risco funcional e setorial.** O risco é associado a funcionalidades específicas (ex: compra, chat aberto) ou conteúdos ilegais. Serviços utilitários (bancos, emprego) ou editoriais são caracterizados como de menor risco ou com regulação própria.	**Risco estrutural e sistêmico.** O risco é associado ao modelo de negócio baseado em engajamento, ao design de interface (rolagem infinita, notificações) e à arquitetura algorítmica. Adota-se a tipologia dos "4Cs" (Conteúdo, Contato, Conduta, Contrato).	**Risco associado à própria solução.** O risco central não é apenas o conteúdo ou o contato, mas a arquitetura de dados criada pela solução de verificação. Preocupação com centralização de dados e potencial uso indevido da infraestrutura.
Demanda de escopo	**Aplicação restrita e proporcional.** Foco em conteúdos legalmente proibidos ou de alto risco. Defesa de tratamento diferenciado para setores já regulados (Financeiro/KYC, Editorial, Profissional).	**Aplicação ampliada ao risco estrutural.** A regulação deve abranger ambientes de interação social e design de engajamento intensivo, independentemente de o conteúdo ser criminalizado. Questionamento da distinção rígida entre conteúdo positivo e negativo em redes abertas.	**Inclusão da fiscalização dos mecanismos.** O escopo da regulação deve incluir a fiscalização dos próprios sistemas de verificação, para evitar que se tornem vetores de coleta excessiva de dados.
Argumento central	**Conformidade prévia e viabilidade econômica.** Argumentos de que setores já cumprem regras próprias (KYC, classificação indicativa); de que exigências uniformes oneram pequenos agentes; de que a regulação deve distinguir entre tipos de serviço.	**Proteção integral e precaução.** Argumentos de que o design de engajamento expõe crianças a riscos; de que conteúdos de diferentes naturezas coexistem nas mesmas plataformas; de que a curadoria algorítmica amplifica exposição a riscos.	**Soberania e privacidade.** Argumentos de que a centralização excessiva cria riscos de vigilância; de que a delegação a grandes plataformas gera dependência tecnológica; de que há risco de ponto único de falha (*single point of failure*).
Posição sobre grandes plataformas	**Eficiência de mercado.** Defesa de que a verificação seja centralizada em Lojas de Apps/Sistemas Operacionais, o que reduziria custos para desenvolvedores menores. Argumento de que isso evita redundância de coleta de dados.	**Responsabilidade proporcional ao poder.** Defesa de que plataformas com maior controle da arquitetura e maior capacidade econômica devem ter obrigações mais rigorosas (*duty of care*) e responsabilidade proporcional.	**Questionamento da centralização.** Oposição à delegação da verificação a um único agente centralizado (seja plataforma privada ou infraestrutura estatal), alertando para riscos de vigilância e dependência.

A leitura horizontal deste quadro demonstra que o debate sobre o escopo não é apenas técnico, mas ontológico:

- Para o Bloco 1, a internet é um conjunto de serviços distintos (um banco é diferente de um TikTok), e a regulação deve respeitar essas fronteiras funcionais para não colapsar a economia digital.

- Para o Bloco 2, a internet de consumo é um ecossistema de captura de atenção, onde o risco é transversal e invisível (algoritmos), exigindo uma regulação que perpasse as definições funcionais de "serviço".

- O Bloco 3 atua como uma "consciência crítica" lateral, alertando que a solução proposta pelos dois primeiros blocos (verificação de idade) pode criar um problema (vigilância), rompendo com a polarização binária "Mercado vs. Proteção" ao introduzir o eixo "Liberdade Civil"

3.3 Eixo 3: Arquitetura da Implementação (ARQ)

3.3.1 Visão geral e definição do eixo

O eixo de Arquitetura da Implementação (ARQ) sintetiza as disputas sobre o local e a frequência da verificação de idade, polarizada entre a defesa da centralização em lojas de aplicativos e sistemas operacionais, com posições divergentes entre a defesa da centralização em lojas de aplicativos, proposta por plataformas digitais com argumentos de eficiência e minimização de dados, e a posição de fabricantes de dispositivos e organizações da sociedade civil. O debate estende-se à temporalidade da validação, opondo o modelo de cadastro único à exigência de verificações a cada acesso para serviços de alto risco, e aborda a distribuição de responsabilidades na cadeia técnica, onde terminologias como "sinais de idade" e "perfis multiusuário" são mobilizadas para definir os limites da obrigação de cada agente no ecossistema digital.

3.3.2 Frequência e relevância dos temas

A distribuição de frequência deste eixo indica uma concentração preponderante de argumentos sobre a definição do *locus* de implementação da verificação, com o código ARQ_LOJA_APPS (28) representando a maior parcela das unidades de conteúdo deste tema, focada na centralização do controle nos níveis de sistema operacional e lojas de aplicativos. Em segundo plano, observa-se a discussão sobre a temporalidade e recorrência da validação, polarizada entre as menções à exigência de checagem a cada interação (ARQ_CADA_ACESSO, 20) e a defesa de validações únicas no momento do registro (ARQ_CADASTRO_UNICO, 13). As limitações técnicas impostas pelo compartilhamento de hardware aparecem no código ARQ_DISPOSITIVO_PART (11), enquanto a atribuição de deveres na ponta final da cadeia é abordada pelos códigos ARQ_APP_LEVEL (10) e ARQ_CADEIA_RESP (9), que somados tratam da responsabilidade de aplicações individuais e outros agentes da cadeia de valor.

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
ARQ_LOJA_APPS	28	Argumentos de que a verificação deveria ocorrer no nível da Loja de Aplicativos ou do Sistema Operacional, centralizando o controle na camada de infraestrutura.
ARQ_CADA_ACESSO	20	Discussões sobre a exigência de verificação "a cada acesso", especialmente para serviços de alto risco.
ARQ_CADASTRO_UNICO	13	Argumentos favoráveis à verificação única no momento do cadastro, sem necessidade de revalidação posterior.
ARQ_DISPOSITIVO_PART	11	Discussões sobre o desafio dos dispositivos compartilhados por múltiplos usuários (ex: famílias), que dificultam a verificação baseada em conta única.
ARQ_APP_LEVEL	10	Argumentos de que a verificação deveria ocorrer no nível da aplicação ou site, permitindo controle contextual pelo desenvolvedor.
ARQ_CADEIA_RESP	9	Discussões sobre a distribuição de responsabilidades na cadeia de valor digital (desenvolvedores, plataformas, lojas de aplicativos, anunciantes).
TOTAL	**91**	

3.3.3 Principais argumentos

A. Centralização na Loja de Apps

A arquitetura que delega a aferição de idade às Lojas de Aplicativos (*App Stores*) e Sistemas Operacionais (SO) emerge como o ponto de maior tensão discursiva, revelando uma clivagem clara entre as grandes plataformas de redes sociais/aplicativos e as organizações da sociedade civil. O argumento central, apresentado por plataformas como a Meta, posiciona esta arquitetura como a "5ª Geração" de soluções, cintando o Radar Tecnológico, onde a eficiência e a privacidade convergem. A Meta argumenta que essa centralização "ajuda a reduzir a proliferação de superfícies de processamento de dados pessoais", defendendo que "pais e responsáveis só precisam verificar a idade do filho uma vez, no nível do dispositivo ou da loja de aplicativos, eliminando a necessidade de verificações de idade repetidas vezes em vários aplicativos". Esta posição é corroborada pelo Match Group (Tinder), que sustenta que "as lojas de aplicativos estão bem posicionadas para melhorar substancialmente a segurança online por meio da restrição de idade no nível da loja de aplicativos.", sugerindo que tal modelo "reduz significativamente a necessidade de processamento extensivo de dados, minimizando as invasões de privacidade".

Contudo, essa transferência de responsabilidade é contestada por atores que apontam falhas estruturais na cobertura desse modelo. A PROTESTE argumenta que limitar a aferição às lojas é insuficiente pois "crianças e adolescentes acessam serviços por diferentes vias, incluindo aplicativos pré-instalados, *Smart TVs*, consoles, dispositivos compartilhados e fluxos alternativos de acesso que não passam pelo controle direto das lojas oficiais". A organização alerta que tal arquitetura "deixa em posição secundária justamente os ambientes onde se encontram os maiores riscos psicossociais […] como plataformas de interação social". O Instituto Alana reforça essa limitação técnica, notando que "nos métodos baseados no dispositivo, a verificação ocorre no próprio equipamento […] sem transmissão direta de dados a terceiros", o que, embora preserve privacidade, pode ser ineficaz se não houver comunicação robusta com a ponta da aplicação.

Há ainda uma resistência técnica por parte dos próprios fabricantes de dispositivos e *marketplaces*. A Roku, por exemplo, traz a experiência internacional para afirmar que “não há viabilidade conceitual em exigir que os sistemas operacionais realizem a aferição de idade”. A Samsung complementa essa visão ao argumentar que “seria demasiadamente custoso exigir que as lojas de aplicativos fossem as responsáveis por aferir a idade, considerando que cada produto ou serviço possuem conteúdos e públicos diversos”. A Microsoft adota uma postura intermediária de minimização, recomendando que “sistemas operacionais não sejam obrigados a coletar dados de categoria de idade além dos seguintes grupos: menores de 13, 13-15, 16-17 e maiores de 18”, e que “a loja não deve ser obrigada a realizar verificação de idade adicional”. Por fim, o Instituto Teckids oferece uma crítica à governança desse modelo, afirmando que, embora centralizado, ele é “arriscado como solução principal […] incompatível com o princípio de governança e proteção integral”.

B. Descentralização no nível do app

Em contraste direto com a centralização nas lojas, há um argumentos que defendem a verificação realizada pela própria aplicação ou site, baseada na premissa de que apenas a aplicação conhece o contexto do risco. A Samsung é taxativa ao defender que “é fundamental que ela ocorra dentro nos aplicativos […] pois garante que o método de aferição de idade esteja adequado ao tipo de conteúdo do aplicativo, seu público-alvo e sua finalidade”. A empresa argumenta que as lojas de aplicativos são insuficientes pois, “ainda que elas realizem a aferição de idade, compras e serviços dentro do aplicativo e anúncios podem expor crianças”.

A Apple, embora controladora de uma loja, posiciona sua solução *Declared Age Range API* como uma ferramenta para empoderar o desenvolvedor, e não para substitui-lo, explicando que “permite que o aplicativo receba a faixa etária da criança sem compartilhar sua data de nascimento”, mantendo a lógica de que os desenvolvedores usam esses sinais para “oferecer experiências de aplicativos adequadas”. O Instituto Alana observa que os métodos baseados na aplicação permitem “recorrer a técnicas como análise comportamental, autenticação federada”, sendo relevantes para definir “o grau de autonomia do usuário”. ITS Rio pondera os prós e contras, notando que “no nível do aplicativo, por exemplo, a verificação tende

a ser mais contextualizada e ajustável, mas também mais vulnerável à autodeclaração fraudulenta".

C. O Problema do dispositivo compartilhado

A realidade socioeconômica brasileira impõe uma barreira crítica às soluções baseadas em dispositivo: o compartilhamento de aparelhos. A Yoti traz dados contundentes ao debate, afirmando que "no Brasil, onde cerca de 41% dos domicílios de baixa renda compartilham um único smartphone […] as configurações no nível do dispositivo, por si só, são insuficientes. A empresa explica que confiar apenas no dispositivo" correm o risco de bloquear o acesso legítimo de adultos ou permitir que crianças contornem as medidas de segurança em dispositivos compartilhados.". O Instituto Alana endossa essa preocupação, notando que a prática familiar de compartilhamento "complica a verificação no dispositivo ou sistema operacional, pois os modelos profundos na *stack* arriscam alienar usuários".

As soluções propostas para este desafio variam entre perfis de usuário e autenticações locais. O Match Group sugere que a verificação em dispositivos partilhados "pode ser alcançada implementando perfis multiusuário com restrições personalizadas baseadas na idade, adaptadas a cada usuário". A Associação Brasileira de Anunciantes (ABA) recomenda a adoção de "configurações padrão em 'modo infantil' ou 'modo seguro', ativadas localmente e desativáveis tão somente mediante PIN ou senha do responsável". O IDEC propõe uma abordagem combinada, onde dispositivos devem oferecer "ferramentas de proteção que não exponham dados de adultos (e.g. senhas específicas para aplicativos, perfis restritos)". Já o FNPETI é categórico ao afirmar que, dado este cenário, "uma autenticação realizada no nível do aparelho é insuficiente para garantir quem está de fato utilizando o serviço em cada sessão".

D. Verificação a cada acesso

Há um consenso quase absoluto no setor privado contra a interpretação literal da exigência de verificação "a cada acesso" (Art. 9º, §1º), classificada como inviável e prejudicial à experiência do usuário, enquanto a sociedade civil defende sua aplicação estrita apenas para contextos de altíssimo risco. A Federação do Comércio de Bens, Serviços e Turismo de SP resume a preocupação econômica, alertando que tal

medida “implicaria elevados investimentos em infraestrutura, aumento do tempo de resposta das plataformas, maior fricção para o usuário e potencial redução da usabilidade”. A Samsung reforça que isso geraria “aumento da possibilidade de burla do mecanismo […] prejudicando a experiência no ambiente digital”. A BRASSCOM expande o argumento para a esfera jurídica, notando que “exigir verificação de idade contínua em cada ponto de acesso e para cada sessão […] não encontra precedentes em outras jurisdições”.

Em contrapartida, atores focados na proteção da infância defendem a medida, mas com escopo cirúrgico. A ABERT esclarece que a verificação a cada acesso é mandatória “quando o usuário tenta acessar conteúdos ou serviços cujo consumo por menores é proibido por lei, como material pornográfico”, argumentando que “somente ela garante que a restrição legal seja cumprida”. O Instituto Alana concorda, especificando que a regra é aplicável a “websites de apostas, pornografia, compras de produtos restritos, onde a exposição […] pode resultar em danos imediatos”.

Uma solução intermediária, baseada em “momentos reais de interação”, é proposta pela PROTESTE e pela Yoti. A PROTESTE sugere que a aferição ocorra em gatilhos como “criação de conta; primeiro acesso; ativação de funcionalidades sensíveis”. A Yoti corrobora tecnicamente essa visão, afirmando que “é lógico que a verificação de idade seja realizada no momento da interação, ou seja, no cadastro ou imediatamente antes do acesso a um recurso com restrição de idade.”. O Fórum Nacional de Prevenção e Erradicação do Trabalho Infantil (FNPETI) introduz uma nuance técnica importante para justificar a recorrência: “um *passkey* serve como um método de autenticação seguro para a sessão, e mantém-se a necessidade de uma nova verificação de idade a cada acesso a um conteúdo de alto risco”.

E. Verificação única no cadastro

Este código agrupa a defesa da eficiência e da minimização de dados através de uma verificação robusta realizada uma única vez, no momento da criação da conta. A Meta é uma defensora vocal deste modelo, argumentando que a estrutura do ECA Digital deve permitir que “os usuários passem pelo processo de verificação de idade uma única vez com um provedor confiável”, o que “elimina a necessidade de jovens e suas famílias enviarem repetidamente documentação sensível”. A eSapiens

concorda, postulando que “a aferição de idade vinculada ao login deve ser considerada método eficiente e suficiente […] dispensando a necessidade de nova verificação em abertura de sessão”.

A Federação do Comércio de SP estabelece uma distinção operacional, afirmando que “em regra, a verificação tende a ser mais adequada no momento da criação de conta”, embora admita exceções para lojas de aplicações. A Family Talks reforça a eficácia deste momento, notando que “ao exigir a verificação etária no processo de criação de contas, a plataforma […] impõe um filtro significativo”. A AMOBITEC adiciona que a reutilização dessa aferição, “como por meio de age tokens, mostra-se muito pertinente, especialmente porque torna desnecessário o processamento excessivo de dados pessoais sensíveis”.

F. Complexidade da cadeia de responsabilidade

O último código aborda a governança sistêmica da verificação, rejeitando a atribuição de responsabilidade a um único elo. O Instituto Alana propõe o uso de “sinal de idade (*age signal*) como um mecanismo complementar, especialmente em arquiteturas distribuídas”, onde a validação gera apenas um sinal criptográfico. A PROTESTE critica a atual estrutura legal que, segundo sua análise, “estabelece deveres específicos quase exclusivamente para sistemas operacionais e lojas de aplicativos”, argumentando que a proteção “não pode depender exclusivamente da atuação dos controladores da porta de entrada tecnológica”.

A visão de responsabilidade compartilhada é ecoada pelo setor privado. O Match Group afirma que “a responsabilidade pela verificação de idade deve ser compartilhada […] entre desenvolvedores de protocolo, desenvolvedores de aplicativos e provedores de infraestrutura”. A Câmara Brasileira da Economia Digital reforça que “em arquiteturas descentralizadas ou federadas, a responsabilidade pela aferição de idade deve ser distribuída conforme o papel técnico e jurídico”. A PROTESTE conclui que serviços de alto risco, como redes sociais e *Video on Demand* (VOD), “devem assumir parcela proporcional da responsabilidade, seja por meio de mecanismos próprios ou pela integração a soluções interoperáveis”.

3.3.4 Terminologia e conceitos-chave

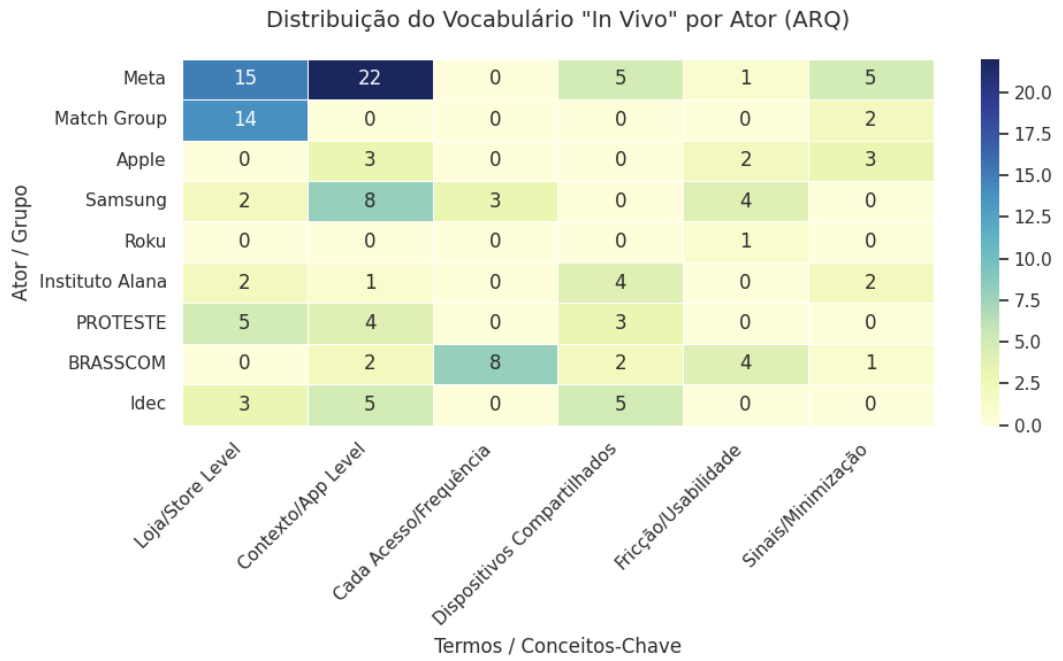
O vocabulário utilizado pelos participantes revela diferentes enquadramentos técnicos. A expressão “Nível da Loja” (*Store Level*) é utilizada por plataformas de conteúdo para descrever uma solução que centraliza a verificação na camada de infraestrutura. A Apple introduz o termo “Sinais de Idade”(*Age Signals*) associado à sua *'Declared Age Range API'*, caracterizando a informação transmitida como indicativa e não determinística.

Do lado da descentralização, a Samsung utiliza o termo “Contexto do Aplicativo” para argumentar que a verificação deve ocorrer onde há conhecimento específico sobre o risco do conteúdo.

A expressão 'Dispositivos Compartilhados' emerge como conceito relevante trazido por organizações da sociedade civil e contribuintes da academia, questionando a premissa de correspondência entre usuário e conta única que fundamenta arquiteturas de identidade digital.

A Figura 3 representa a visualização de dados gerada a partir da análise quantitativa do vocabulário identificado na interpretação qualitativa.

Figura 3: Temas dos principais atores sobre arquitetura



Fonte: produção própria

Esta matriz de calor demonstra empiricamente a dissidência discursiva mapeada, mostrando como cada ator “carrega” nos termos que sustentam sua arquitetura de poder preferida.

Quadro Comparativo: Posições sobre Arquitetura de Implementação (ARQ)

GRUPO DE CONTRIBUINTES	ARQUITETURA PREFERIDA	ARGUMENTO CENTRAL	POSIÇÃO SOBRE RESPONSABILIDADE
Provedores de Aplicação de Conteúdo	**Centralizada na Loja/Sistema Operacional**	Argumentam que a centralização é mais eficiente e segura, evitando fragmentação de dados. Para aplicações com riscos de interação pessoal, destacam a importância de verificação por agente externo à plataforma.	Defendem que a verificação seja realizada pela camada de infraestrutura (lojas de aplicativos, sistemas operacionais), com a aplicação consumindo o sinal de idade já validado.
Fabricantes de Hardware e Infraestrutura	**Descentralizada no nível da Aplicação**	Argumentam que o Sistema Operacional não possui contexto sobre o conteúdo específico de cada aplicação. Uma regra uniforme na loja poderia ser excessivamente restritiva para alguns casos ou insuficiente para outros.	Defendem que a responsabilidade pela verificação recaia sobre a aplicação que oferece o conteúdo, cabendo ao hardware apenas fornece recursos técnicos neutros.

GRUPO DE CONTRIBUINTES	ARQUITETURA PREFERIDA	ARGUMENTO CENTRAL	POSIÇÃO SOBRE RESPONSABILIDADE
Provedores de Sistema Operacional	**Híbrida / Ferramentas opcionais**	Argumentam que podem fornecer ferramentas técnicas (APIs de sinal de idade) sem assumir papel de verificador universal. Enfatizam a minimização de dados como princípio orientador.	Defendem modelo em que o sistema operacional fornece meios técnicos, mas a decisão de aplicação e a responsabilidade pelo resultado permanecem com o desenvolvedor da aplicação.
Sociedade Civil e Academia	**Verificação recorrente / Por sessão**	Argumentam que a arquitetura técnica deve refletir a realidade de uso (dispositivos compartilhados por famílias). A verificação única no cadastro não protege quando múltiplos usuários acessam o mesmo dispositivo.	Defendem que a verificação ocorra em momentos-chave de acesso a conteúdo de risco, garantindo que o usuário atual seja, de fato, o titular autorizado.

3.4 Eixo 4: Soluções Técnicas e Métodos (TECH)

3.4.1 Visão geral e definição do eixo

O Eixo de SOLUÇÕES TÉCNICAS E MÉTODOS (TECH) consolida o debate sobre as ferramentas de implementação da verificação, polarizado entre modelos baseados em tratamento de dados biométricos, infraestrutura estatal e protocolos criptográficos. Os participantes divergem sobre a natureza da estimativa facial, definida por fornecedores e plataformas como inferência estatística anônima distinta da identificação, enquanto organizações da sociedade civil a classificam como coleta de dados sensíveis que exige exclusão imediata. A verificação documental é descrita como método acessível no contexto nacional, porém associada a riscos de segurança no armazenamento, o que fundamenta a defesa do uso de bases governamentais (Gov.br) para centralizar a custódia e eximir empresas de responsabilidade. Em contrapartida, ZKPs são apontadas como técnica de minimização de dados, embora o setor produtivo alegue inviabilidade econômica para sua adoção massiva. As grandes plataformas tecnológicas propõem o uso de inferência comportamental via Inteligência Artificial e controles parentais no nível do sistema operacional, abordagens contestadas por outros atores devido à necessidade de monitoramento contínuo da atividade do usuário e à presunção de letramento digital familiar, restando à autodeclaração, ao uso de dados financeiros e à validação por terceiros

independentes o papel de alternativas para contextos de menor risco ou serviços transacionais.

3.4.2 Frequência e relevância dos temas

A distribuição de frequência do eixo de Soluções Técnicas (TECH) evidencia uma divisão equitativa no topo da hierarquia temática, com os códigos *TECH_ESTIMATIVA_FACIAL* e *TECH_ZKP_TOKEN* registrando o mesmo número máximo de ocorrências (21 unidades cada), o que indica um equilíbrio entre a discussão sobre métodos de análise biométrica e a proposição de tecnologias de preservação de privacidade via criptografia. Logo em seguida, o código *TECH_GOV_INFRA* (17) consolida o uso de infraestruturas estatais como a terceira via predominante de implementação. Em um nível intermediário de relevância, observam-se as abordagens de inferência comportamental (*TECH_INFERENCIA_IA*, 11) e verificação documental tradicional (*TECH_DOC_OFICIAL*, 10), enquanto os métodos baseados em delegação de controle (*TECH_CONTROLE_PARENTAL*, 7) e autodeclaração (*TECH_AUTODEC_VALIDA*, 6) ocupam posições secundárias. As soluções setoriais específicas, como o uso de dados bancários (*TECH_DADO_BANCARIO*, 3) e validadores externos (*TECH_TERCEIRO_VALIDADOR*, 2), representam a parcela residual da amostra.

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
TECH_ESTIMATIVA_FACIAL	21	Discussões sobre biometria, reconhecimento facial e estimativa de idade por análise de imagem.
TECH_ZKP_TOKEN	21	Discussões sobre tecnologias de preservação de privacidade (Prova de Conhecimento Zero — *Zero Knowledge Proof*), tokens anonimizados e credenciais verificáveis.
TECH_GOV_INFRA	17	Discussões sobre uso de bases de dados governamentais (Gov.br, SERPRO, Receita Federal) como fonte de validação de identidade e idade.
TECH_INFERENCIA_IA	11	Discussões sobre análise comportamental, histórico de navegação e inferência algorítmica de idade por inteligência artificial.
TECH_DOC_OFICIAL	10	Discussões sobre verificação documental tradicional (envio de RG, CNH ou Passaporte).

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
TECH_CONTROLE_PARENTAL	7	Discussões sobre ferramentas que delegam a validação aos pais ou responsáveis (vínculo de contas, aprovação de downloads).
TECH_AUTODEC_VALIDA	6	Discussões sobre autodeclaração de idade, incluindo argumentos favoráveis e contrários, frequentemente proposta como camada inicial em modelos escalonados.
TECH_DADO_BANCARIO	3	Discussões sobre uso de informações bancárias ou de cartão de crédito (*Open Banking*) para verificar maioridade civil.
TECH_TERCEIRO_VALIDADOR	2	Discussões sobre recurso a birôs de crédito, empresas de verificação de identidade (*ID Techs*) ou validadores privados externos.
TOTAL	**98**	

3.4.3 Principais argumentos

A. Estimativa facial

Os dados indicam uma batalha discursiva fundamental sobre a natureza da estimativa facial. Os fornecedores de tecnologia e plataformas argumentam que a estimativa facial não constitui identificação pessoal, caracterizando-a como dado de entrada para cálculo estatístico que não é armazenado. A Yoti é a protagonista desta construção, apresentando a definição técnica de que sua ferramenta realiza a “análise de uma imagem para inferir a idade sem identificar ou reconhecer qualquer indivíduo”. Ao enfatizar que o sistema “apaga imediatamente a imagem assim que a idade é estimada”, a empresa busca neutralizar o temor do armazenamento biométrico, argumentando que o dado deixa de existir quando a função é cumprida. Para a Yoti, assim como os demais provedores de tecnologias de aferição de idade, essa tecnologia não é vigilância, mas sim inclusão, pois “oferece uma opção inclusiva para pessoas que não possuem documento de identidade.”, posicionando a face como o “documento dos desdocumentados”.

A eSapiens e o Match Group (Tinder) aderem a essa narrativa, enquadrando a “biometria regulada” como uma das soluções mais promissoras para “equilibrar precisão e privacidade”. O Match Group vai além, sugerindo que a estimativa facial elimina a necessidade de documentos sensíveis, reduzindo o risco de vazamento de dados (honeypots). A Roblox traz uma aplicação prática que transcende o acesso,

utilizando a estimativa para “garantir experiências apropriadas” e limitar interações, argumentando que a tecnologia já opera como moderadora de convivência em sua plataforma, não apenas porteira.

Em contrapartida, o Instituto Alana e a AMOBITEC recusam a higienização semântica do termo. Para o Alana, independentemente de se chamar “estimativa” ou “reconhecimento”, trata-se de “método altamente invasivo” que coleta dados biológicos únicos de crianças. O Instituto impõe condições estritas para sua aceitabilidade, exigindo garantias de que a imagem “não seja usada para treinar o algoritmo” e que haja o “expurgo imediato”. A AMOBITEC reforça que, devido à sua intrusividade, este método deve ser “restrito a casos de alto risco”, rejeitando sua banalização como padrão de acesso para a internet como um todo.

B. Infraestrutura governamental

A infraestrutura estatal emerge como opção nas contribuições, com diferentes argumentos favoráveis à sua adoção. A Family Talks, por exemplo, defende pragmaticamente a integração com o “login Gov.br”, argumentando que se deve “aproveitar a base já existente” da Identificação Civil Nacional (ICN) para evitar a duplicidade de esforços e custos. A lógica aqui é de eficiência operacional: por que criar sistemas se o Estado já validou a identidade de milhões?

O Match Group (Tinder) apoia essa via por uma razão jurídica defensiva. Ao afirmar que a verificação “devem ser centralizadas em bancos de dados seguros e gerenciados pelo governo”, a empresa busca transferir para o Estado o ônus da custódia de dados sensíveis. Se o governo valida, a plataforma se exime da responsabilidade de armazenar documentos. Contudo, essa dependência da infraestrutura estatal é vista com reserva por outros atores, como Zetta e BRASSCOM, que (conforme explorado no eixo RISC) temem que a centralização em plataformas como Gov.br crie um “ponto único de falha” e facilite a vigilância, defendendo que o Estado deve ser uma opção, não o monopólio da verificação.

C. Prova de conhecimento zero e *tokens*

Existe uma tensão entre o ideal ético da criptografia e a realidade material do mercado brasileiro. Diversas associações da sociedade civil, sendo o principal representante o Instituto Alana, consideram as provas de conhecimento zero (*zero-knowledge proofs* - ZKP) como o "padrão ouro para verificação de atributos". A construção de sentido aqui é baseada na minimização absoluta, já que a tecnologia permite provar "que a pessoa possui determinado atributo (ser maior de 18 anos) sem revelar a identidade". A BRASSCOM reconhece teoricamente essa superioridade, admitindo que "soluções como tokens verificáveis… garantem anonimato seletivo", o que resolveria o paradoxo privacidade/segurança.

No entanto, a própria BRASSCOM analisa sua aplicabilidade prática, introduzindo o argumento da inviabilidade econômica. A associação alerta que "tais tecnologias ainda são inacessíveis para muitas empresas brasileiras", especialmente Pequenas e Médias Empresas (PMEs), sugerindo que impor o "padrão ouro" geraria exclusão de mercado. A Strima tenta preencher essa lacuna entre o ideal e o real propondo a adoção da norma "ISO/IEC 27566" como roteiro de implementação, argumentando que a padronização internacional pode baixar o custo de entrada. A Intervozes alinha-se à defesa dos tokens como ferramenta de "autodeterminação informativa", vendo na criptografia uma forma de devolver o controle do dado ao usuário, contrastando com o modelo de custódia das plataformas.

D. Autodeclaração validada

A autodeclaração, frequentemente tratada como ineficaz, como anteriormente identificado, é defendida vigorosamente pela Roku e pela Câmara-e.net como uma camada necessária de usabilidade. A Roku argumenta que, para uma TV na sala, a autodeclaração é uma solução de "baixo impacto" que permite configurar o ambiente sem fricção excessiva. A PROTESTE concorda, mas com ressalvas: ela serve para "contextos de baixo risco".

A inovação proposta pela Câmara Brasileira da Economia Digital é o conceito de "autodeclaração assistida" ou "validada". Não se trata apenas de perguntar a idade, mas de cruzar essa declaração com "sinais de inconsistência". Se o usuário diz ter 18 anos mas consome conteúdo infantil ou usa vocabulário infantil, o sistema

detecta a anomalia. É uma tentativa de salvar a autodeclaração através da inteligência de dados.

E. Inferência por IA

A inferência por IA é apresentada pela Meta como a alternativa “sem atrito” e “sem documento”. A empresa detalha o uso de “tecnologia de análise de texto no Instagram” e “predição de idade, alimentada por IA”, construindo a idade não como um dado biológico ou documental, mas como um padrão de comportamento digital. A Federação do Comércio de SP endossa essa abordagem, sugerindo a “análise de consistência do comportamento” como forma de validar autodeclarações sem exigir upload de RG.

O contra-argumento, articulado principalmente pela sociedade civil como Instituto Alana e FNPETI, é que essa solução técnica é, na verdade, “um problema de privacidade amplificado”, já que “para inferir a idade pelo comportamento, a plataforma precisa monitorar tudo o que o usuário faz, diz e clica.” O FNPETI denuncia que esse modelo “opera por meio de uma vigilância contínua”, criando um “perfilamento” que é ilegal perante o ECA. Assim, o que a Meta vende como “menos intrusivo” (porque não pede foto), a sociedade civil classifica como “mais invasivo” (porque vigia a conduta).

F. Documentos oficiais

A verificação documental é o campo onde a desigualdade social brasileira se torna argumento técnico. A Samsung, por exemplo, defende o uso de documentos oficiais cruzados com bases públicas (como a Receita Federal) não apenas por segurança, mas por “acessibilidade”. O argumento da empresa é que, num país desigual, o RG é mais universal do que “smartphones com câmeras de alta resolução” necessários para biometria facial de qualidade. Para a Samsung, a tecnologia de ponta pode ser excludente, enquanto a burocracia estatal é inclusiva.

Instituições da sociedade civil como o Instituto Alana e a Coalizão Direitos na Rede, contudo, apontam o risco de segurança dessa materialidade. O armazenamento de cópias de documentos cria os “honeypots” mais perigosos. O Match Group concorda, afirmando que “empresas… enfrentam riscos

significativos” ao manusear esses documentos, reforçando sua preferência por delegar essa tarefa ao governo. A Yoti posiciona o documento como uma falha de privacidade, pois ele “revela mais dados do que o necessário (nome, endereço, filiação)”, violando o princípio da minimização, enquanto a estimativa facial revelaria apenas a idade.

G. Dados bancários e terceiros validadores privados

O uso de dados financeiros é defendido pela eSapiens e pela Strima especificamente para o setor de serviços pagos (streaming, compras). O argumento é pragmático: o sistema financeiro já realizou o Know Your Customer (KYC) rigoroso. Se o usuário possui um cartão de crédito válido, a presunção de maioridade é forte e o custo de verificação é zero para a plataforma. O Instituto Alana aceita essa premissa, sugerindo o aproveitamento de “verificações pregressas de bancos e operadoras de telecomunicações como forma de reduzir a coleta de novos dados”, aplicando o princípio da economia de dados.

Atores como AMOBITEC e Yoti trazem a solução arquitetural das ID Techs. A proposta é a interposição de um “terceiro de confiança” entre o usuário e a plataforma. A Yoti cita o modelo francês da ARCOM para explicar o conceito de “independência jurídica e técnica”: o verificador vê o documento, mas não sabe onde o usuário vai navegar; a plataforma vê que o usuário é adulto, mas não sabe quem ele é (não vê o documento). A AMOBITEC defende esse modelo para evitar que plataformas de mobilidade ou serviços diversos precisem montar seus próprios departamentos de verificação, criando um mercado especializado de identidade.

I. Ferramentas de controle parental

Ainda uma das tecnologias mencionadas é o suporte de controle parental associado à estratégia das empresas de hardware e sistemas operacionais (Apple, Microsoft) de deslocar a verificação da “nuvem” para a “borda” (dispositivo). A Apple descreve sua “*Declared Age Range API*” como uma ferramenta que “empodera os pais” sem expor a criança às plataformas. A lógica é: o pai configura o iPhone, e o iPhone avisa ao app “este usuário é criança”, sem dizer quem é. A Microsoft reforça essa abordagem de categorização ampla (faixas etárias) em vez de datas exatas.

Para a Zetta, essa abordagem é ideal pois descentraliza o risco e respeita a dinâmica familiar. Contudo, críticos na Sociedade Civil apontam que isso pressupõe pais digitalmente letrados e dispositivos de uso exclusivo, ignorando a realidade brasileira de dispositivos compartilhados e pais com baixa literacia digital (lacuna identificada no eixo IMPACT).

3.4.4 Terminologia e conceitos-chave

A terminologia utilizada pelos participantes para descrever a materialidade das ferramentas de verificação, revelando uma disputa semântica onde a escolha das palavras define a aceitabilidade ética e a viabilidade econômica da tecnologia. O vocabulário demonstra que o campo é estruturado por uma tensão entre a linguagem da "precisão" estatística e a linguagem da "invasão" biométrica, bem como entre a "segurança" da infraestrutura estatal e a "autodeterminação" dos protocolos criptográficos.

O tratamento da imagem facial é objeto de caracterizações divergentes entre os contribuintes. Os fornecedores de tecnologia e plataformas utilizam sistematicamente o termo "estimativa etária" em vez de "reconhecimento facial", preferindo sistematicamente o léxico da "estimativa etária" (*age estimation*) e da "inferência". A Yoti Ltd. e a eSapiens utilizam termos como "análise de uma imagem" (*analysis of an image*) e "biometria regulada" para descrever o processo, enfatizando a "exclusão imediata" (*deleting the image*) e a ausência de "identificação" (*without identifying*). Este vocabulário caracteriza a imagem como um dado efêmero e estatístico, dissociado da identidade civil. Em contrapartida, o Instituto Alana e a AMOBITEC recusam essa distinção, insistindo no uso de termos como "dado biométrico sensível", "método altamente invasivo" e "coleta de PII" (*Personally Identifiable Information*). Para estes atores, a tecnologia é descrita através do vocabulário do risco e da intrusão, exigindo "expurgo imediato" e garantias contra o "treinamento de algoritmos", termos que denotam uma desconfiança profunda sobre o uso secundário dos dados biológicos.

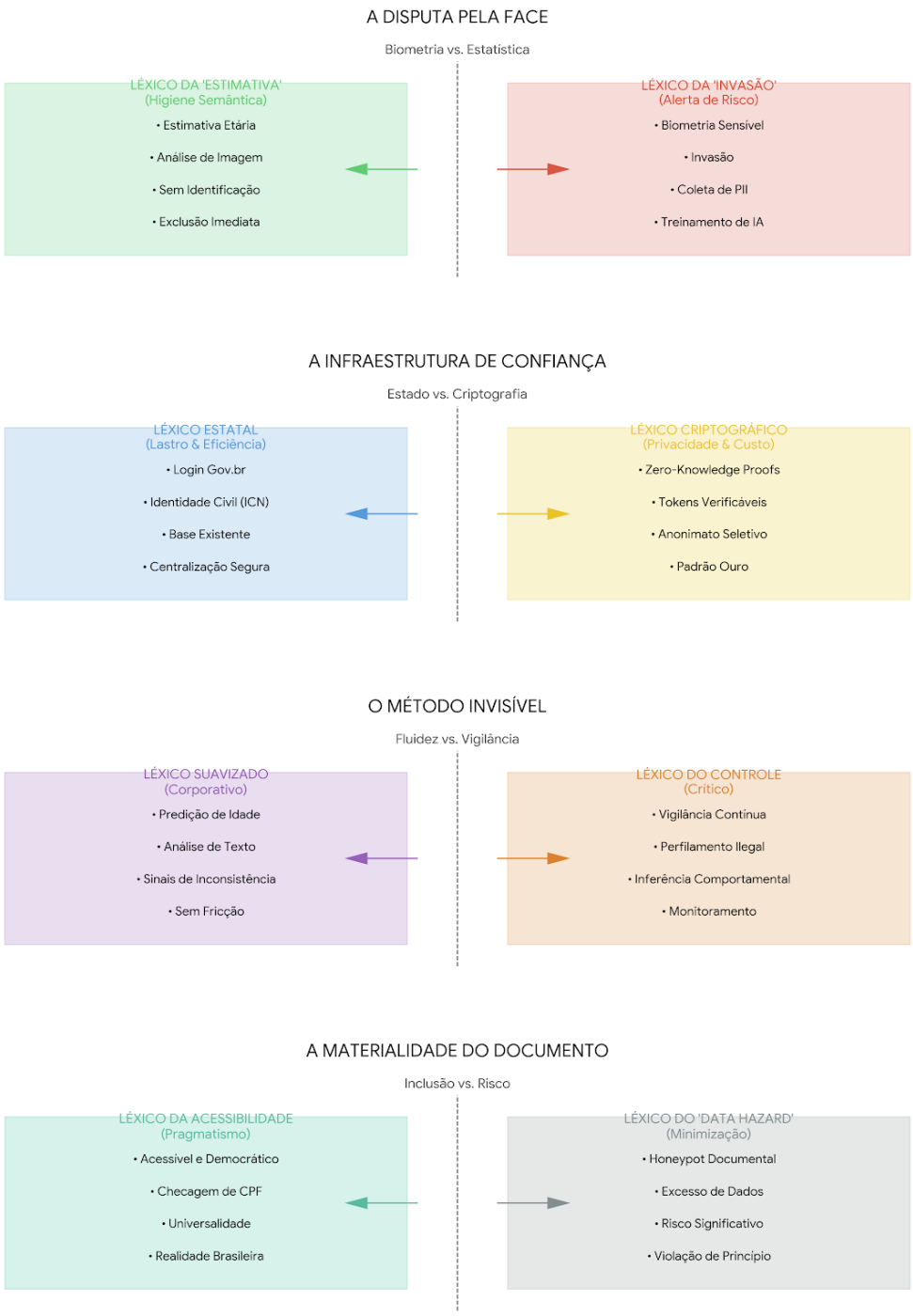
A infraestrutura de verificação é descrita através de um léxico que oscila entre a eficiência burocrática e a blindagem matemática. A defesa do modelo estatal mobiliza termos institucionais como "Identidade Civil Nacional (ICN)", "login Gov.br" e "bases

governamentais". A Family Talks e o Match Group utilizam vocabulário de gestão, falando em "aproveitar a base já existente" e "centralização segura", onde o Estado é descrito como o ente capaz de suportar o ônus da custódia. No polo oposto, o léxico da criptografia introduz termos técnicos de *Privacy by Design*. Instituto Alana e a BRASSCOM empregam expressões como "provas de conhecimento zero" (*zero-knowledge proofs* - ZKP), "tokens verificáveis" e "anonimato seletivo". O conceito de "atributo" é central aqui: a tecnologia permite provar um atributo (ser maior de idade) sem revelar a "identidade". Contudo, a BRASSCOM introduz o vocabulário da exclusão econômica, classificando essas soluções como "inacessíveis" para o mercado local, contrapondo o "padrão ouro" técnico à realidade do "custo Brasil".

A descrição dos métodos comportamentais e de autodeclaração revela um léxico de fricção e vigilância. A Meta e a Federação do Comércio de SP utilizam termos suavizados como "análise de texto", "predição de idade" e "sinais de inconsistência" para descrever o monitoramento da atividade do usuário. A idade não é verificada, mas "inferida" a partir do "comportamento". O FNPETI, entretanto, traduz esses termos técnicos para o vocabulário da violação de direitos, classificando-os como "vigilância contínua" e "perfilamento", vedados pela legislação. A autodeclaração é descrita pela Roku e Câmara-e.net através do léxico da usabilidade: é uma solução de "baixo impacto" e "alto alcance", necessária para evitar a fricção em contextos de baixo risco.

Por fim, a materialidade do documento oficial é descrita de forma ambivalente. Enquanto a Samsung utiliza o vocabulário da inclusão, defendendo a "checagem de CPF" e o "documento oficial" como meios "acessíveis" e "democráticos" em contraste com smartphones caros, a Yoti e o Match Group descrevem o mesmo objeto através do léxico do perigo de dados (*data hazard*), alertando que o documento físico revela "mais dados do que o necessário" e cria "riscos significativos" de vazamento. A solução proposta pela AMOBITEC e Yoti introduz a terminologia da "independência", onde "terceiros de confiança" (ID Techs) operam um modelo de separação de dados, garantindo que a plataforma não acesse o documento do usuário. A Figura 4 apresenta uma síntese das diferentes caracterizações tecnológicas.

Figura 4: Síntese da divisão do discurso sobre tecnologias



Fonte: produção própria

Quadro Comparativo: Posições sobre Soluções Técnicas (TECH)

DIMENSÃO DE ANÁLISE	SETOR PRIVADO	SOCIEDADE CIVIL E ACADEMIA	POSIÇÕES INTERMEDIÁRIAS OU DIVERGENTES
Biometria e Estimativa Facial	**Fornecedores de tecnologia** argumentam que a estimativa facial é distinta do reconhecimento facial, caracterizando-a como análise estatística de dado temporário, sem armazenamento de identidade. Defendem que a tecnologia pode ser implementada com privacidade por design.	**Organizações de direitos digitais** classificam qualquer tratamento de imagem facial como dado biométrico sensível, exigindo expurgo imediato e vedação de uso para treinamento de IA.	**Associações setoriais** (ex: AMOBITEC) alinham-se às preocupações sobre riscos da biometria, defendendo restrição a contextos de alto risco, diferentemente da posição de fornecedores especializados.
Infraestrutura Governamental (Gov.br)	**Parte do setor privado** manifesta preocupação com dependência de infraestrutura estatal única, citando riscos de ineficiência e ponto único de falha. Preferem soluções de mercado descentralizadas ou múltiplos provedores.	**Parte da sociedade civil** defende o uso da infraestrutura Gov.br para aproveitar base de dados existente (ICN), evitando custos duplicados e novas coletas de dados sensíveis.	**Algumas plataformas** defendem centralização governamental como forma de transferir a custódia de dados sensíveis para o Estado, que teria maior capacidade de segurança.
Inferência por IA e Comportamento	**Plataformas** defendem a inferência de idade via análise de texto e comportamento como solução de baixa fricção que dispensa documentos ou biometria. Argumentam que é menos intrusiva por não exigir envio de dados adicionais.	**Organizações de direitos digitais** argumentam que a inferência comportamental exige monitoramento contínuo da atividade do usuário, caracterizando-a como forma de vigilância que pode violar princípios de proteção de dados.	—
Documentos Oficiais	**Fornecedores de verificação** apontam riscos de segurança no armazenamento de cópias de documentos, preferindo métodos que não exijam retenção de imagens de RG ou CNH.	**Organizações de direitos digitais** concordam com o risco de armazenamento, vendo o envio de documentos como violação do princípio da minimização. Preferem métodos que verifiquem apenas o atributo de idade.	**Fabricantes de hardware** argumentam que documentos oficiais são mais acessíveis que tecnologias dependentes de câmeras de alta resolução, considerando a realidade de desigualdade de acesso a dispositivos.
Criptografia (*Zero-Knowledge Proofs*)	**Associações setoriais** reconhecem a qualidade técnica das ZKPs, mas argumentam que o custo de implementação é elevado para pequenas e médias empresas, defendendo que	**Organizações de direitos digitais** defendem as ZKPs como padrão preferencial por garantir verificação de atributo sem revelação de identidade, atendendo	**Contribuintes do setor de padronização** propõem adoção de normas ISO internacionais para viabilizar a tecnologia em escala, reduzindo custos através de padronização.

DIMENSÃO DE ANÁLISE	SETOR PRIVADO	SOCIEDADE CIVIL E ACADEMIA	POSIÇÕES INTERMEDIÁRIAS OU DIVERGENTES
	não seja exigência obrigatória.	ao princípio da minimização de dados.	

3.5 Eixo 5: Argumentos de Legitimação (LEGIT)

3.5.1 Visão geral e definição do eixo

Este eixo agrupa os argumentos utilizados pelos contribuintes para fundamentar suas posições regulatórias. A análise identificou cinco categorias principais de argumentação: (i) conformidade prévia com marcos legais existentes; (ii) inclusão social como justificativa para determinadas tecnologias; (iii) experiência do usuário como valor a ser preservado; (iv) desenvolvimento de infraestrutura nacional; e (v) valor social dos serviços oferecidos.

3.5.2 Frequência e Relevância dos Temas

A distribuição de frequência da categoria Argumentos de Legitimação (LEGIT) indica uma concentração majoritária de unidades no código *LEGIT_JA_CUMPRO* (14), o qual reúne argumentos que sustentam a suficiência dos mecanismos atuais de conformidade com a LGPD e o ECA para contestar a necessidade de novas regulações. O segundo agrupamento mais relevante, *LEGIT_BIOMETRIA_INCL* (10), articula a defesa de tecnologias biométricas através da ótica da inclusão social, posicionando-as como alternativas mais democráticas que a exigência de documentos oficiais. A tensão entre segurança e navegação é representada pelo código *LEGIT_PRIORIDADE_UX* (7), que centraliza a defesa da fluidez da experiência do usuário em detrimento de barreiras de verificação que gerem fricção. Completam a categoria os temas de escopo geopolítico e moral, com o código *LEGIT_SOBERANIA* (5) focando na defesa de soluções tecnológicas nacionais para evitar dependência externa, e o código *LEGIT_VALOR_SOCIAL* (2) apresentando argumentos de exceção baseados na natureza educativa ou benéfica do conteúdo das plataformas.

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
LEGIT_CONFORMIDADE	14	Argumentos de que as empresas já cumprem a legislação vigente (LGPD, ECA) e que novas regras seriam redundantes ou desnecessárias.
LEGIT_INCLUSAO	10	Argumentos de que tecnologias biométricas promovem inclusão social por não exigirem documentos oficiais, sendo acessíveis a populações sem documentação formal.
LEGIT_EXPERIENCIA	7	Argumentos de que a usabilidade e a fluidez da navegação devem ser consideradas na regulamentação, evitando fricção excessiva para o usuário.
LEGIT_INFRAESTRUTURA	5	Argumentos favoráveis ao desenvolvimento de soluções brasileiras de verificação, reduzindo dependência de infraestrutura tecnológica estrangeira.
LEGIT_VALOR_SOCIAL	2	Argumentos de que determinadas plataformas oferecem conteúdo educativo ou benefícios sociais que justificariam tratamento regulatório diferenciado.
TOTAL	**38**	

3.5.3 Principais argumentos

A. Argumento de conformidade prévia

Contribuintes do setor privado apresentaram argumentos de que os mecanismos existentes de conformidade já seriam suficientes para a proteção pretendida. A Apple listou suas ferramentas de controle parental ("Tempo de Uso", "Pedir para Comprar", "*Made for Kids*") para argumentar que já oferece "uma ampla gama de ferramentas líderes de mercado voltadas para proteger crianças". A empresa sustentou que "sempre priorizou a proporcionalidade e a minimização de dados, evitando demandas excessivas".

Claro S.A. e Samsung apresentaram argumentos similares, sustentando que "a resposta adequada não está na padronização de solução única, mas na aplicação consistente das regras já existentes". Para esses contribuintes, eventual lacuna regulatória residiria na fiscalização das normas vigentes (LGPD, ECA Digital), e não na ausência de obrigações.

A Meta argumentou que utiliza "dados existentes sem ter que solicitar mais dados para verificar a idade", apresentando a inferência comportamental como

"camada adicional de aferição" compatível com os princípios de minimização de dados.

B. Argumentos de inclusão social

Contribuintes do setor de verificação de identidade e algumas plataformas apresentaram argumentos de que determinadas tecnologias, especialmente a estimativa facial, promoveriam inclusão social ao dispensar a apresentação de documentos oficiais.

A Yoti invocou "os 4Ds da inclusão — Documentos, Dispositivos, Deficiência e Diversidade" para argumentar que a exigência de documentos oficiais excluiria populações vulneráveis, sustentando que a "estimativa da idade facial pode servir como uma alternativa simples e que preserva a privacidade". A Meta apresentou argumento similar, citando que a predição de idade seria inclusiva para "aproximadamente um bilhão de pessoas que globalmente não possuem documentos formais".

Por outro lado, o Instituto Alana e a Internet Society (ISOC Brasil) contestaram essa caracterização, argumentando que soluções biométricas "geram um risco significativo ao coletar dados pessoais sensíveis de todos os usuários" e que a inclusão genuína requer "alternativas não biométricas". A Câmara Brasileira da Economia Digital ponderou que a "aplicação indiscriminada pode criar barreiras desnecessárias, amplificar desigualdades", sugerindo que métodos mais robustos sejam reservados para contextos de alto risco.

C. Argumentos sobre infraestrutura nacional

Contribuintes apresentaram argumentos favoráveis ao desenvolvimento de soluções de verificação baseadas em infraestrutura pública brasileira. Daniel Teixeira Bezerra (contribuinte da sociedade civil) argumentou que a aferição de idade deve ser "instrumento de soberania nacional", defendendo o desenvolvimento de infraestrutura pública para que o país não dependa de "serviços que lucram com a coleta de dados pessoais".

O Instituto Alana alinhou-se a essa perspectiva, defendendo "APIs de acesso cego a registros governamentais" como forma de manter a "soberania nacional de

dados". O argumento apresentado é de que a dependência de tecnologias de verificação fornecidas por empresas estrangeiras constituiria vulnerabilidade a ser considerada na formulação da política pública.

D. Prioridade da experiência do usuário

Contribuintes do setor privado apresentaram argumentos de que a preservação da usabilidade constitui valor relevante a ser considerado na regulamentação. A Associação Brasileira de Anunciantes (ABA) argumentou que a verificação rigorosa a cada acesso geraria "custos elevados, aumento da latência, redução da usabilidade e da fluidez". A AMOBITEC sustentou que a proteção não deve "comprometer o direito fundamental de acesso à informação".

A Meta argumentou que sua solução de "predição de idade" oferece "experiência rápida e contínua", contrastando-a com soluções documentais que gerariam "maior atrito e complexidade". A Federação do Comércio de SP propôs a "inferência contínua" como forma de "conciliar a necessidade de segurança com a usabilidade".

A BRASSCOM invocou a LGPD para argumentar que a "coleta reiterada de dados" necessária para verificações frequentes "contraria o princípio da minimização".

E. Valor social dos serviços

Alguns contribuintes apresentaram argumentos de que a natureza de seus serviços justificaria tratamento regulatório diferenciado. A Roblox argumentou ser "única neste aspecto" por oferecer "milhares de experiências educacionais", sustentando que barreiras de idade rígidas poderiam impedir o acesso a benefícios pedagógicos.

O Match Group (Tinder) argumentou que seu modelo de negócio "não se trata de manter os usuários conectados para gerar receita com anúncios direcionados", buscando diferenciar-se de plataformas baseadas em economia da atenção.

3.5.4 Terminologia e conceitos-chave

A análise do vocabulário utilizado pelos contribuintes nesta categoria revela diferentes enquadramentos para fundamentar posições no debate regulatório.

No campo da conformidade legal, contribuintes do setor de telecomunicações e hardware utilizam expressões como "regime rigoroso de conformidade" para qualificar sua situação jurídica atual, reforçada pela expressão "aplicação consistente" das regras existentes. A Apple classifica suas soluções proprietárias como "ferramentas líderes de mercado". Em contrapartida, contribuintes da academia e da sociedade civil utilizam termos como "ineficiente" para descrever padrões estrangeiros atuais (como a COPPA) e propõem o conceito de "soberania nacional de dados". Observa-se que o princípio da "proteção de dados" é invocado por diferentes setores para fundamentar posições distintas: contribuintes do setor privado enfatizam a "minimização de dados" para questionar novas coletas, enquanto contribuintes da academia enfatizam a necessidade de "infraestrutura pública" para garantir autonomia nacional.

A tecnologia biométrica é objeto de caracterizações divergentes. Provedores de tecnologia de identidade e plataformas utilizam termos como "inclusão", "acesso" e "equidade" para descrever ferramentas de estimativa facial. A expressão "alternativa que preserva privacidade e reduz fricção" é utilizada para caracterizar essas tecnologias, enquanto a observação de que "nem todos têm acesso a passaportes" é mobilizada para questionar a exigência documental. Em sentido diverso, contribuintes da sociedade civil utilizam termos como "risco significativo" e "superfície de ataque", posicionando as "alternativas não biométricas" como imperativo de segurança.

A relação entre usabilidade e proteção é caracterizada de formas distintas pelos contribuintes. Associações setoriais e plataformas utilizam termos técnicos de design como "usabilidade", "fluidez" e "latência", chegando a invocar o "direito fundamental de acesso à informação" para questionar barreiras de verificação. O termo "fricção" é utilizado com conotação negativa, associado a "custos elevados" e "barreiras desnecessárias". Plataformas de conteúdo específico utilizam termos como "experiências educacionais" para caracterizar seus serviços, ou diferenciam-se ao afirmar que seu modelo não visa "manter usuários conectados indefinidamente".

O quadro a seguir apresenta a distribuição dos principais argumentos por setor, identificando convergências e divergências entre os contribuintes.

.

Quadro Comparativo: Argumentos de Legitimação (LEGIT)

CATEGORIA	SETOR PRIVADO	SETOR PRIVADO (ID TECHS)	SOCIEDADE CIVIL	ACADEMIA
Conformidade prévia	Ênfase em ferramentas existentes e adesão à LGPD	—	Questionamento da eficácia das medidas atuais	Análise de lacunas normativas
Inclusão social	Inferência como alternativa a documentos	Biometria como solução para indocumentados	Defesa de alternativas não biométricas	Análise de vieses algorítmicos
Experiência do usuário	Usabilidade como valor central	Baixa fricção como diferencial	Proteção não deve ser sacrificada por conveniência	Equilíbrio entre valores
Infraestrutura nacional	Preferência por padrões globais	Alinhamento com certificações internacionais	Defesa de soluções públicas soberanas	Análise de dependência tecnológica
Valor social	Natureza educativa/profissional como atenuante	—	Contestação de exceções setoriais	Análise caso a caso

3.6 Eixo 6: Adequação e Proporcionalidade (ADEQ)

3.6.1 Visão geral e definição do eixo

O Eixo de ADEQUAÇÃO E PROPORCIONALIDADE (ADEQ) agrupa os argumentos normativos sobre o que constitui uma medida “proporcional” ou “adequada”. Ela reúne argumentos normativos que condicionam a escolha dos métodos de verificação de idade ao princípio da proporcionalidade, estabelecendo que a robustez do mecanismo deve corresponder ao nível de risco oferecido pelo serviço digital. A análise dos dados indica um consenso sobre a necessidade de uma abordagem escalonada, na qual métodos rígidos e intrusivos são reservados para contextos de alto risco, como pornografia e jogos de azar, enquanto a autodeclaração é defendida para serviços de baixo risco visando a preservação da usabilidade e do

acesso. Paralelamente, os atores argumentam que a solução tecnológica é insuficiente se não for acompanhada por políticas de educação digital e mediação parental, além de enfatizarem a obrigatoriedade da minimização de dados para evitar práticas de vigilância, apontando as tecnologias de Prova de Conhecimento Zero (ZKP) como o padrão técnico para alinhar verificação e privacidade e demandando alternativas de validação presencial ou assistida para mitigar a exclusão digital.

3.6.2 Frequência e relevância dos temas

A distribuição de frequência da categoria Adequação (ADEQ) evidencia uma concentração de argumentos em torno do princípio da proporcionalidade baseada no risco, com o código *ADEQ_BAIXO_RISCO_FLEX* (25) liderando a amostra ao defender a aplicação de métodos simplificados para contextos de menor ameaça, seguido em paridade estatística pela demanda por verificações robustas exclusivamente em cenários críticos (*ADEQ_ALTO_RISCO_RIGO*, 23). Esta lógica de gradação opera em conjunto com a ênfase na proteção de dados, demonstrada pela igual recorrência do código *ADEQ_MINIMIZACAO* (23), que estabelece a estrita economia de coleta como critério condicionante para a validade de qualquer método. O reconhecimento das limitações da intervenção puramente técnica manifesta-se no código *ADEQ_EDUCACAO* (16), que situa o letramento midiático como requisito de eficácia. As frequências equivalentes dos códigos *ADEQ_OFFLINE_INCL* (13) e *ADEQ_PRIV_ZKP* (13) indicam que as preocupações com a inclusão digital de desconectados e com a implementação de arquiteturas de privacidade criptográfica ocupam posições simétricas na base da hierarquia temática.

CÓDIGO	OCORRÊNCIAS	DESCRIÇÃO BREVE
ADEQ_BAIXO_RISCO_FLEX	25	Argumentos de que serviços de baixo risco devem estar sujeitos a métodos de verificação simplificados ou de menor fricção.
ADEQ_ALTO_RISCO_RIGO	23	Argumentos de que serviços de alto risco devem estar sujeitos a verificação robusta ou documental.
ADEQ_MINIMIZACAO	23	Argumentos favoráveis à coleta mínima de dados, limitada ao estritamente necessário para a verificação de idade.
ADEQ_EDUCACAO	16	Argumentos de que soluções técnicas são insuficientes sem políticas complementares de educação midiática e digital.
ADEQ_OFFLINE_INCL	13	Argumentos favoráveis a mecanismos de validação presencial ou assistida para evitar exclusão digital de populações vulneráveis.

CÓDIGO	OCORRÊNCIAS	DESCRIÇÃO BREVE
ADEQ_PRIV_ZKP	13	Argumentos de que arquiteturas baseadas em Prova de Conhecimento Zero (ZKP) são a solução preferencial para conciliar verificação e privacidade.
TOTAL	**113**	

3.6.3 Principais argumentos

A. Rigor para alto risco

A construção de sentido neste argumento articula-se em torno da premissa da proporcionalidade: a robustez do método deve escalar com o risco. O CGI.br estabelece a base normativa ao afirmar que “a aferição de idade deve ser aplicada ao apenas quando houver risco concreto a segurança”, destacando que a “proporcionalidade um princípio central” busca o equilíbrio “entre grau de risco e robustez”.

A definição de “alto risco” é tecnicamente detalhada por diversos atores. A Strima aponta para “serviços de conteúdo gerado por usuários (UGC), onde há efetiva exposição a conteúdos não classificados”. A Coalizão Direitos na Rede e a BRASSCOM especificam que “em serviços de alto risco, como plataformas de conteúdo adulto e apostas, é justificável adotar métodos mais robustos”. A Claro S.A. e a Samsung concordam com essa classificação, citando “plataformas de conteúdo adulto, apostas ou jogos com interação aberta” como ambientes que justificam “coleta mais ampla de dados”.

O Instituto Alana introduz a necessidade de uma exigência mais rigorosa para esses contextos, com base em critérios adicionais, defendendo que “sejam utilizados mecanismos de autenticação confiáveis a cada acesso, vedando-se o uso exclusivo da autodeclaração”, e alertando que a “interação, especialmente entre crianças e adultos… configura risco elevado”. A PROTESTE expande o escopo do alto risco para incluir “sistemas baseados em recomendação intensiva e serviços de conteúdo adulto”, argumentando que esses serviços devem assumir “parcela proporcional da responsabilidade”.

Do lado do setor privado, a Zetta adverte, ainda, que, embora o risco justifique rigor, “mecanismos excessivamente rígidos podem elevar custos, criar fricção”,

defendendo uma “análise de risco, não em padronização tecnológica”. A Camara-e.net propõe um “modelo graduado de risco” para evitar que métodos intrusivos como documentos oficiais ou biometria sejam usados indiscriminadamente, devendo ser reservados a “contextos de alto risco, como pornografia”.

B. Flexibilidade para baixo risco

Há um consenso de que a baixa fricção é vital para a viabilidade da economia digital e a inclusão. O CGI.br reitera a necessidade de “soluções mais simples e menos invasivas serem priorizadas em contextos de baixo risco”. A eSapiens propõe técnicas específicas de bloqueio parcial, como “desabilitação de funcionalidades interativas” ou “aplicação de blur”, argumentando que são “instrumentos eficazes” sem restringir todo o site.

A defesa da autodeclaração para baixo risco é robusta no setor privado. A Zetta e a Roku argumentam que para serviços como streaming editorialmente controlado, um modelo que “não exija a coleta de documentos adicionais ou dados pessoais, é suficiente”. A Camara-e.net complementa que a autodeclaração, “embora insuficiente para cenários de alto risco, pode funcionar como camada inicial”.

Atores como a Apple invocam documentos da própria autoridade reguladora (ANPD) para sustentar que “exigir que cada pessoa que queira baixar um aplicativo forneça informações pessoais… é prejudicial à privacidade”. A Claro S.A. e a Federação do Comércio de SP utilizam o argumento jurídico da LGPD, afirmando que “métodos simplificados, de menor coleta de dados, tendem a ser mais adequados aos princípios da necessidade e minimização”. A AMOBITEC sugere que em plataformas de menor risco, a aferição ocorra apenas “no momento da compra… permitindo que o restante do serviço permaneça acessível”.

O Instituto Alana, embora rígido no alto risco, concede que para a maioria das plataformas (redes sociais, jogos), devem ser priorizadas “soluções menos intrusivas… que confirmem apenas a faixa etária necessária”.

C. Princípio da minimização

A minimização de dados emerge como o princípio ético e legal (LGPD) que deve reger a arquitetura técnica. A Apple é enfática ao declarar que prioriza a minimização,

o que significa “coletar e usar apenas o mínimo necessário… evitando demandas excessivas”. A Microsoft reforça que qualquer coleta deve ser realizada em “conformidade com limitações rigorosas de finalidade”, vedando o processamento para outros propósitos.

O Instituto Alana vislumbra um modelo onde a verificação gera “apenas um sinal criptográfico indicando a faixa etária… sem compartilhamento de dados pessoais”, o que preservaria a “usabilidade da experiência digital”. A PROTESTE adverte contra a normalização da vigilância: “a coleta de documentos oficiais, biometria… não pode se tornar padrão”.

A Meta descreve sua “API de Idade” como uma solução desenhada com privacidade na essência, onde “nenhuma outra informação do usuário, nem mesmo a data de nascimento, é transmitida para os aplicativos”. O Google também defende a “minimização razoável de dados”, alertando contra a obrigatoriedade de “ferramentas que envolvam o processamento de dados pessoais desnecessários”. A AMOBITEC e a Camara-e.net alertam especificamente contra o risco da biometria, notando que pode haver “coleta de dados pessoais sensíveis de forma desproporcional à atividade primária”.

D. Necessidade de educação digital

A interpretação deste eixo revela a insuficiência da solução puramente técnica. O Instituto Teckids argumenta que a solução “mais robusta, segura e realista para dispositivos compartilhados é garantir a existência de perfis de uso separados”, deslocando a responsabilidade para a configuração do dispositivo.

A Kaspersky aponta a falibilidade técnica, notando que “muitos menores contornam controles de idade com conhecimento ou apoio de adultos”, concluindo que “conscientização e educação digital são tão importantes quanto barreiras técnicas”. A Claro S.A. e a Federação do Comércio de SP concordam que “políticas públicas de educação digital… são necessárias e indispensáveis para complementar os esforços empresariais”.

O Instituto Alana propõe uma estratégia midiática ampla, sugerindo a “promoção de campanhas de conscientização multimídia… envolvendo artistas, comunicadores”,

além de incluir o tema nos currículos escolares (BNCC). Em seu documento anexo, reforçam que a educação é estratégica para “fortalecer a autonomia informada das famílias e reduzir a dependência exclusiva de soluções tecnológicas que são imperfeitas”. A Camara-e.net resume a posição ao afirmar que “aferição de idade não substitui políticas de educação digital… qualquer modelo de verificação será limitado se não integrado a estratégias de literacia digital”.

E. Inclusão *offline*

A preocupação com a exclusão digital é central neste argumento. A Yoti apresenta a contribuição mais estruturada, propondo que o Brasil adote um modelo onde “cidadãos sem evidência documental… deveriam poder usar um cartão de prova de idade dedicado”, além de sugerir “quiosques seguros em correios” para quem não tem smartphone.

O CTS-FGV (Academia) sugere a “verificação presencial” (*In-Person Validation*) em locais como PROCONs, onde um terceiro emitiria uma chave criptográfica, facilitando o acesso para “pessoas com dificuldades de acesso à internet”. Eles também propõem o “Atestado Social” (*Social Vouching*), onde “professores, assistentes sociais… poderiam atestar a idade”.

O Ministério Público Federal (MPF) corrobora a necessidade de “mecanismos alternativos” como “formulários físicos ou serviços presenciais em órgãos públicos (Cartórios, Correios, CRAS)”. O Instituto Alana reforça a ideia de “*Onboarding* Presencial” em “escolas, CRAS, bibliotecas”, argumentando que isso amplia o alcance social. A Internet Society (ISOC Brasil) alerta que tecnologias dependentes de câmeras e conexão estável podem excluir “idosos, pessoas com deficiência, populações rurais e comunidades indígenas”.

F. ZKP Como melhor garantia de privacidade

A tecnologia de *Zero Knowledge Proof* (ZKP) foi apontada por diversos contribuintes como solução preferencial para conciliar verificação e privacidade.. O FNPETI descreve a arquitetura preferível: uso da infraestrutura pública (identidade digital) para emitir credenciais que, através de ZKP, permitem “comprovar a idade sem compartilhar dados pessoais”. O Instituto Alana afirma que as ZKPs “representam a

melhor alternativa para a privacidade, pois resolvem o conflito entre eficácia e proteção de dados".

O Ministério Público Federal (MPF) concorda que métodos ZKP oferecem o "melhor equilíbrio", implementando "anonimato desde a concepção". A Unico - IDTech cita o exemplo europeu (EDI Wallets) que utiliza ZKP para estabelecer um "novo padrão de privacidade".

Empresas como a Meta e o Google mencionam o desenvolvimento de APIs e "credenciais digitais" que operam sob lógicas similares de minimização. O Match Group (Tinder) defende especificamente "tokens de preservação de privacidade emitidos por lojas de aplicativos" como o melhor equilíbrio. A DiraCom sintetiza que o método de "emissão de certificação criptografada… por Prova de Conhecimento Zero" é o que melhor preserva os dados pessoais.

3.6.4 Terminologia e conceitos-chave

A terminologia utilizada para articular as tensões entre segurança, privacidade e acesso revela que a discussão sobre adequação não opera sobre categorias binárias simples, mas sobre um gradiente semântico onde o termo "proporcionalidade" atua como o operador central de legitimidade. O CGI.br e a Zetta empregam este termo para exigir um equilíbrio entre o "grau de risco" e a "robustez" da medida, estabelecendo uma taxonomia onde a exigência de verificação é condicionada à existência de "risco concreto" ou "dano significativo". A definição do que constitui esse risco mobiliza termos específicos: a Strima e a Samsung referem-se à exposição a "conteúdos não classificados" e à "interação aberta em ambientes de UGC" (Conteúdo Gerado pelo Usuário) como gatilhos para mecanismos mais rígidos. Por outro lado, a PROTESTE expande o léxico do risco para incluir sistemas de "recomendação intensiva", enquanto a Coalizão Direitos na Rede delimita o "alto risco" a setores como "jogos de azar" e "conteúdo adulto".

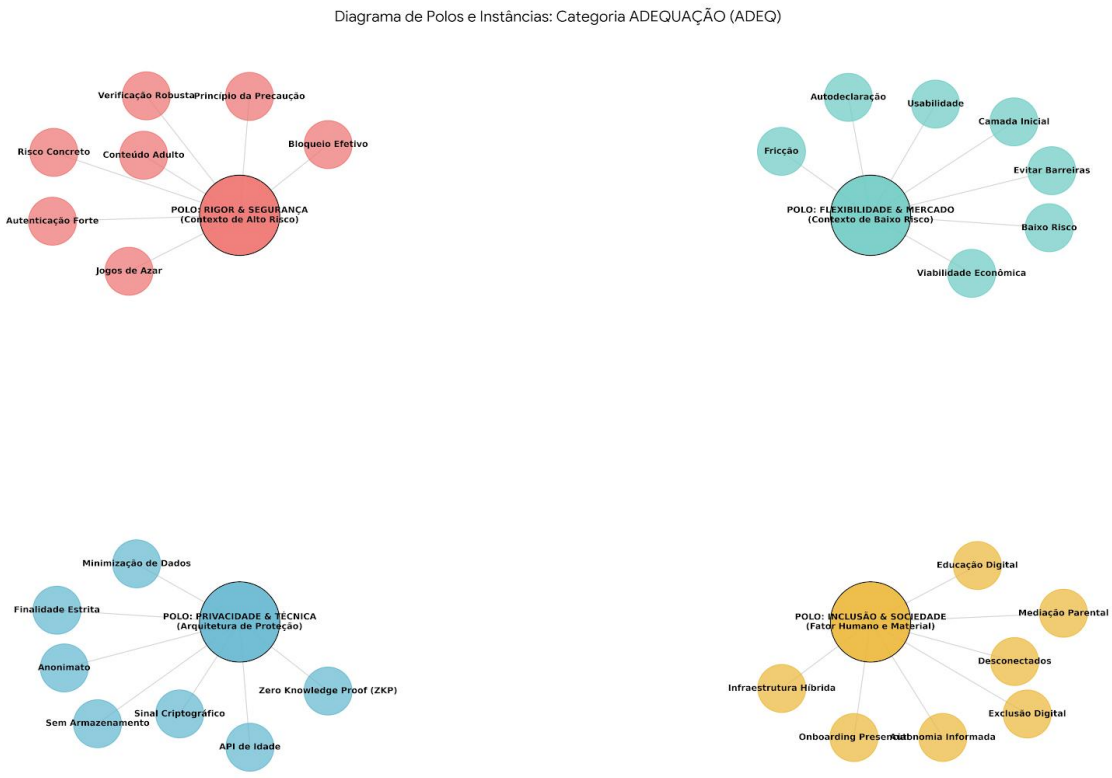
No campo semântico das soluções técnicas, observa-se uma disputa vocabular entre a "fricção" e a "autodeclaração". Atores do setor privado, como Roku e Zetta, utilizam termos como "barreiras de inclusão", "custos excessivos" e "fricção" para descrever os efeitos indesejados de métodos rígidos em serviços de baixo risco. A "autodeclaração" é resignificada não como uma ausência de verificação, mas, nas

palavras da Camara-e.net, como uma “camada inicial” ou, segundo a Claro S.A., um “método simplificado” adequado aos princípios da “necessidade”. Em contraste, o Instituto Alana introduz o termo “autenticação confiáveis” para opor-se à autodeclaração em contextos de risco, exigindo provas de vida ou documental. A eSapiens contribui com um vocabulário de modulação técnica, sugerindo a “desabilitação de funcionalidades” ou a aplicação de “blur” (borramento) como alternativas ao bloqueio total, indicando uma preferência por intervenções granulares.

A gramática da privacidade é dominada pelo termo “minimização”, extraído diretamente do arcabouço legal da LGPD e operacionalizado tecnicamente pelos participantes. A Apple e a Microsoft utilizam a expressão “mínimo necessário” para delimitar a coleta de dados, enquanto o Instituto Alana e a Meta descrevem a solução ideal através de termos como “sinal criptográfico”, “API de Idade” e “tokens”, enfatizando que a verificação deve resultar em um output binário (sim/não) e não na transferência de identidade. O léxico atinge maior especificidade técnica com a introdução do termo “Zero Knowledge Proof” (ZKP) ou “Prova de Conhecimento Zero”. O MPF, a DiraCom e o FNPETI apropriam-se deste vocabulário para descrever um estado de “anonimato desde a concepção”, onde “credenciais verificáveis” permitem a comprovação de atributos sem a revelação de dados brutos. O Match Group reforça essa terminologia ao citar “tokens de preservação de privacidade”, consolidando a ZKP como o significante mestre para a solução do paradoxo privacidade-segurança.

Finalmente, a dimensão sociotécnica introduz um vocabulário voltado para a materialidade do acesso e a competência humana. O termo “exclusão digital” é frequentemente associado aos “desconectados” ou àqueles sem “evidência documental”, conforme notado pela Internet Society e pelo Yoti. Para mitigar esse fenômeno, surgem termos que descrevem infraestruturas híbridas: “quiosques seguros”, “cartão de prova de idade” e “*onboarding* presencial” em “CRAS” ou “escolas”. O CTS-FGV introduz o conceito de “Atestado Social” (*Social Vouching*) e “validação presencial”, ampliando o léxico da verificação para além do digital. Paralelamente, a ineficácia técnica é descrita através de termos como “contornam controles” (Kaspersky), o que demanda soluções baseadas em “letramento digital”, “conscientização” e “autonomia informada”, deslocando a ênfase da ferramenta para a “mediação parental” e a “educação”.

Figura 5: Síntese dos temas em cada polo dos discursos sobre adequação



Fonte: produção própria

A Figura 5 mostra o Diagrama de Polos e Instâncias, projetado para espacializar as quatro grandes vertentes discursivas que organizam o eixo ADEQUAÇÃO E PROPORCIONALIDADE (ADEQ). Este diagrama isola os polos do debate, permitindo visualizar claramente quais conceitos orbitam em torno de cada lógica fundamental. O diagrama divide o campo fenomenológico em quatro quadrantes distintos, cada um representando uma lógica normativa e operacional específica identificada nos dados

1. **Polo: Rigor & Segurança (Quadrante Superior Esquerdo - Vermelho)** - Lógica: Representa a demanda por controle estrito diante de ameaças severas. - Instâncias: Aqui residem conceitos como “Verificação Robusta” e “Autenticação Forte”. Note que estas instâncias são justificadas pela presença de “Risco Concreto” (como “Conteúdo Adulto” e “Jogos de Azar”) e operam sob o “Princípio da Precaução”. É o polo da barreira alta.

2. **Polo: Flexibilidade & Mercado (Quadrante Superior Direito - Turquesa)**

- Lógica: Representa a defesa da fluidez econômica e da experiência do usuário em contextos de menor ameaça.
- Instâncias: Este polo agrupa conceitos como “Autodeclaração” (validada aqui como “Camada Inicial”) e “Baixo Risco”. O vocabulário central gira em torno da “Viabilidade Econômica” e da redução de “Fricção”, visando garantir a “Usabilidade” e evitar barreiras desnecessárias.

3. **Polo: Privacidade & Técnica (Quadrante Inferior Esquerdo - Azul)**

- Lógica: Foca na arquitetura ética da solução, priorizando a proteção de dados sobre a identificação civil.
- Instâncias: As instâncias aqui são soluções técnicas para o anonimato: “Zero Knowledge Proof (ZKP)”, “Sinal Criptográfico” e “API de Idade”. O princípio regente é a “Minimização de Dados” e a “Finalidade Estrita”, buscando provar a idade “Sem Armazenamento” de identidade.

4. **Polo: Inclusão & Sociedade (Quadrante Inferior Direito - Amarelo)**

- Lógica: Aborda as limitações materiais da tecnologia e a necessidade de competência humana.
- Instâncias: Reconhece a “Exclusão Digital” e a existência de “Desconectados”. As soluções instanciadas são híbridas (“Infraestrutura Híbrida”, “*Onboarding* Presencial”) ou comportamentais (“Educação Digital”, “Mediação Parental”), enfatizando a “Autonomia Informada” em vez do bloqueio técnico puro.

Esta visualização demonstra que a discussão sobre adequação não é linear, mas sim uma negociação constante entre estes quatro polos: quanto mais se move em direção ao Rigor, mais se distancia da Flexibilidade; quanto mais se prioriza a Técnica pura, mais se corre o risco de ignorar a Inclusão Social se não houver medidas compensatórias.

Quadro Comparativo: Posições sobre Adequação e Proporcionalidade (ADEQ)

DIMENSÃO DE ANÁLISE	SETOR PRIVADO (Plataformas, Associações e Advocacia)	SOCIEDADE CIVIL E ACADEMIA	CONTRIBUINTES COM ÊNFASE TÉCNICA (ID Techs e Especialistas)
Concepção de Proporcionalidade	**Proporcionalidade como viabilidade:** A proporcionalidade é invocada para calibrar exigências conforme o modelo de negócio e preservar a experiência do usuário. A análise de risco é proposta como critério para diferenciar níveis de exigência, evitando regras uniformes.	**Proporcionalidade como garantia:** A proporcionalidade é invocada como mecanismo de equilíbrio entre proteção da criança e não-invasão da privacidade. Defende-se intervenção robusta onde o risco é concreto, com foco na eficácia da proteção.	**Proporcionalidade como arquitetura:** A proporcionalidade é associada à escolha do ponto de verificação na cadeia técnica (hardware, intermediários, aplicação), com foco em onde a verificação ocorre, não apenas em sua intensidade.
Posicionamento sobre Autodeclaração	**Autodeclaração para baixo risco:** Defesa da autodeclaração para serviços de baixo e médio risco (ex: streaming, e-commerce), argumentando que, combinada com controle parental, atende aos requisitos de melhores esforços e minimização de dados.	**Restrição da autodeclaração:** Questionamento da autodeclaração como método isolado para ambientes de alto risco (ex: redes sociais, jogos interativos). Argumenta-se que a facilidade de evasão compromete a eficácia da proteção, exigindo verificação de atributos para serviços críticos.	**Verificação por atestado:** Proposta de substituição da autodeclaração por atestado criptográfico emitido por terceiro ou pelo dispositivo, desvinculando a verificação da declaração individual do usuário.
Arquitetura Tecnológica Preferencial	**Soluções internas:** Preferência por soluções proprietárias ou APIs internas que realizam estimativa ou inferência de idade dentro do ecossistema da plataforma, evitando compartilhamento com terceiros externos.	**Privacidade por design (ZKP):** Defesa de tecnologias de Prova de Conhecimento Zero e protocolos descentralizados. A arquitetura deve garantir anonimato desde a concepção, impedindo que a verificação se converta em infraestrutura de rastreamento.	**Segregação de camadas:** Proposta de que a verificação ocorra no nível do dispositivo (hardware/OS) ou através de intermediários neutros (ID Techs), isolando a identidade do acesso ao conteúdo e criando silos de dados.
Abordagem sobre Educação e Inclusão	**Educação como complemento:** A educação digital e a mediação parental são apresentadas como complementos à verificação técnica. Ênfase na responsabilidade compartilhada entre plataforma e família.	**Educação como política estruturante:** A educação é proposta como política pública estruturante. Introduz-se a dimensão da exclusão material, exigindo alternativas presenciais/assistidas para populações vulneráveis e desconectadas.	**Capacitação técnica do usuário:** Foco na autonomia técnica do usuário para configurar dispositivos e gerenciar perfis de uso separados (perfil infantil vs. adulto) no hardware.

Obs.: A coluna CONTRIBUINTES COM ÊNFASE TÉCNICA captura as nuances identificadas na análise microanalítica (ex: ID Techs como Unico e a perspectiva de Hardware do Instituto Teckids) que

não se alinham perfeitamente nem com a defesa comercial irrestrita, nem com a regulação de conteúdo tradicional.

3.7 Eixo 7: Riscos Específicos (RISC)

3.7.1 Visão geral e definição do eixo

O Eixo de RISCOS ESPECÍFICOS (RISC) sintetiza os argumentos sobre as vulnerabilidades sistêmicas e ameaças à privacidade introduzidas pela aferição de idade conforme percebido pelos participantes, centralizando-se nas preocupações manifestadas de que a infraestrutura técnica possa ser utilizada para vigilância estatal ou monitoramento de cidadãos, ou desviada para mineração comercial, perfilamento publicitário e treinamento não autorizado de modelos de Inteligência Artificial. Os atores identificam a centralização de dados sensíveis como vetor de criação de alvos prioritários para ataques cibernéticos (*honeypots*), dada a heterogeneidade na maturidade de segurança das empresas, e apontam o risco de reidentificação de usuários anônimos através do cruzamento de metadados e inferências sobre estruturas familiares. Simultaneamente, as unidades de conteúdo descrevem a facilidade técnica de evasão das medidas por meio de ferramentas como VPNs e *deepfakes*, o que comprometeria a eficácia da norma ao deslocar usuários para jurisdições não reguladas sem garantir a proteção pretendida

3.7.2 Frequência e relevância dos temas

A distribuição de frequência da categoria Riscos e Ameaças (RISC) apresenta uma concentração primária no código *RISC_VIGILANCIA_ESTADO* (12), que reúne a maior parcela das unidades focadas na possibilidade de cooptação da infraestrutura de verificação para fins de monitoramento governamental e controle social. Em um segundo nível de incidência, observa-se uma paridade entre os riscos associados à segurança e à finalidade econômica dos dados, com os códigos *RISC_HONEYPOT* (7) e *RISC_MINERACAO_COMERCIAL* (7) abordando, respectivamente, a vulnerabilidade de bases centralizadas a ataques externos e o desvio de informações coletadas para perfilamento publicitário. O segmento restante da amostra distribui-se de maneira uniforme, registrando 6 ocorrências para cada um dos códigos finais, os quais tratam da falibilidade técnica dos sistemas frente a ferramentas de evasão (*RISC_EFICACIA_EVASAO*), da possibilidade de quebra de anonimato via cruzamento de metadados (*RISC_REID_CRUZADA*) e do uso não

autorizado de dados para o treinamento de modelos de Inteligência Artificial (*RISC_TREINO_IA*).

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
RISC_VIGILANCIA_ESTADO	12	Preocupações de que a infraestrutura de verificação possa ser utilizada para vigilância em massa, controle estatal ou rastreamento de cidadãos.
RISC_HONEYPOT	7	Preocupações com a criação de bases de dados centralizadas que se tornam alvos prioritários para ataques cibernéticos e vazamentos (efeito *honeypot*).
RISC_MINERACAO_COMERCIAL	7	Preocupações com desvio de finalidade, onde dados coletados para verificação de idade sejam utilizados para perfilamento publicitário ou comercial.
RISC_EFICACIA_EVASAO	6	Questionamentos sobre a eficácia da verificação diante de possibilidades técnicas de evasão (uso de VPNs, *deepfakes*, documentos falsos).
RISC_REID_CRUZADA	6	Preocupações com reidentificação de usuários anônimos através do cruzamento de metadados técnicos e padrões de navegação.
RISC_TREINO_IA	6	Preocupações com o uso não autorizado de dados biométricos ou comportamentais para treinamento de modelos de Inteligência Artificial.
TOTAL	**44**	

3.7.3 Principais argumentos

A. Vigilância estatal

Os dados revelam o temor de que a infraestrutura de proteção infantil seja cooptada para fins de controle social. A Coalizão Direitos na Rede estabelece a premissa fundamental de que “o propósito da aferição de idade não deve ser o de promover vigilância ou controle sobre jovens”, um posicionamento normativo que busca desvincular proteção de monitoramento. O Instituto Alana aprofunda essa preocupação ao alertar que, “sem transparência… sistemas de aferição podem ser percebidos como instrumentos de controle ou censura”, vinculando a legitimidade da medida à confiança pública. O ator argumenta que a implementação deve “vedar práticas de vigilância massiva ou identificação compulsória”, invocando o ECA Digital como barreira jurídica.

A DiraCom intensifica a crítica ao citar a Electronic Frontier Foundation (EFF), ponderando que “os riscos são de tal monta que os sistemas de verificação etária se constituem como ‘sistemas de vigilância’”. Para este ator, a vigilância não é um efeito colateral, mas a natureza intrínseca da tecnologia proposta. O CGI.br corrobora essa visão estrutural ao afirmar que a verificação “não pode resultar, inadvertidamente, em vigilância massiva… ou na criação de registros de navegação associados à identidade civil”.

Parte do setor privado, representado pela Zetta, alinha-se a essa retórica de direitos civis, argumentando que a implementação “não pode, sob o pretexto de proteger os menores, criar um aparato de vigilância que monitore a atividade de todos os cidadãos”, classificando tal possibilidade como “inconstitucional”. A Strima expande o cenário de risco para além do Estado democrático, alertando que esses dados podem “levar a usos não autorizados por governos autoritários… para perseguir dissidentes”. O FNPETI foca na vigilância comercial, descrevendo a análise comportamental como o “método mais invasivo, operando por meio de uma vigilância contínua da atividade do usuário”.

B. *Honeypots* e vazamentos

A fenomenologia do *honeypot* descreve a inevitabilidade do vazamento em sistemas centralizados. A Zetta introduz o termo ao prever que, “na falta de soluções públicas… o setor privado seria forçado a criar bases de dados gigantescas… gerando ‘*honeypots’* extremamente atrativos para cibercriminosos”. O Instituto Alana concorda, detalhando que a coleta de PII (Informações Pessoais Identificáveis) cria um “alvo de alto valor” que pode “expor milhões de crianças a roubo de identidade”. O Instituto adiciona uma camada de realidade econômica ao risco, notando que “muitas empresas no Brasil podem não ter infraestrutura… adequada”, citando dados da ICTS Protiviti de que “71,9% das micro e pequenas empresas ainda não mapearam dados pessoais”.

O Instituto Teckids reforça a crítica arquitetural, afirmando que a solução “acaba por armazenar estes dados em grandes bancos de dados centralizados que se tornam alvos prioritários”. A Internet Society - Capítulo Brasil complementa que a centralização cria “pontos únicos de falha”, ampliando a superfície de ataque.

Em contraste com a posição majoritária de rejeição à centralização, o Match Group propôs a centralização em infraestrutura governamental, argumentando que o Estado teria maior capacidade de custódia segura de dados sensíveis: “deveria ser centralizado em bancos de dados seguros e gerenciados pelo governo… para reduzir o potencial de violações de dados.”. Para este ator, o Estado é visto como um porto seguro, enquanto para os atores locais e a sociedade civil, a centralização (seja pública ou privada) é o próprio risco.

C. Treinamento de IA sem consentimento

O risco mais emergente refere-se ao uso não consentido de dados para treinar modelos de Inteligência Artificial. A eSapiens identifica o perigo de que “imagens ou vídeos coletados para estimativa facial sejam utilizados indevidamente para treinar modelos de IA proprietários”. A DiraCom reforça que há um “alto risco de que a verificação etária seja usada como pretexto para a coleta massiva… visando o refinamento de tecnologias de reconhecimento facial”.

A Family Talks demanda que a autoridade “proíba explicitamente o uso de dados biométricos de crianças para o treinamento”, uma posição ecoada pela PROTESTE, que veda qualquer “exploração econômica” desses dados para “treinamento de algoritmos”. Uma contribuinte acadêmica inclui este risco no rol de “usos secundários… sem a devida transparência”. A AMOBITEC, representando o setor de mobilidade e tecnologia, concorda com a cautela, alertando para evitar que “dados sensíveis alimentem bases de treinamento de IA sem controle”.

D. Mineração comercial de dados

A preocupação central aqui é a monetização dos dados de segurança. O Instituto Alana define o conflito de interesses: “interesses comerciais das plataformas (perfilamento para publicidade…) podem conflitar com a minimização de dados”. O ator exige salvaguardas contratuais para impedir o “enriquecimento de perfil comercial”. A PROTESTE é categórica ao afirmar que “dados coletados exclusivamente para aferição de idade não podem ser cruzados com bases de marketing”.

Uma contribuinte acadêmica descreve o risco como “uso secundário dos dados”, alertando para a “criação de perfis comportamentais para publicidade direcionada”. A Câmara Brasileira da Economia Digital (camara-e.net), defendendo o setor, tenta delimitar a proibição, argumentando que “o ECA Digital não proíbe a coleta de dados, mas sim o seu uso para fins comerciais… direcionados a crianças”, sugerindo que a coleta para segurança é legítima desde que não alimente o *ad-tech*. No entanto, a AMOBITEC pede cautela com a inferência comportamental, pois ela pode levar “à coleta excessiva… desproporcional à atividade primária”.

E. Reidentificação cruzada

Este argumento aborda a quebra de privacidade através da inferência, não da identificação direta. A Strima explica o mecanismo técnico: “informações coletadas para verificação… podem ser cruzadas com histórico de navegação, permitindo a reidentificação”. Uma contribuinte acadêmica aponta um risco específico para a estrutura familiar: “a vinculação indireta de contas de menores a perfis de pais… permitindo inferências sobre a estrutura familiar”.

A Family Talks exige que a autoridade garanta que “metadados técnicos… não permitam a reidentificação”, enquanto a Microsoft admite explicitamente o risco inerente à sua própria indústria: “A garantia de idade… cria um risco de reidentificação… pois associa a atividade online a uma identidade do mundo real”. A PROTESTE alerta que “mesmo métodos leves podem gerar inferências indevidas”, exigindo “tecnologias baseadas em credenciais verificáveis” para impedir a criação de um “grafo social” do usuário. O Instituto Alana prescreve a norma “ISO/IEC 27556” como padrão técnico necessário para mitigar esse risco.

F. Evasão e ineficácia

Este argumento desconstrói a crença na infalibilidade tecnológica. A eSapiens utiliza o caso do Reino Unido como prova empírica de falha, relatando que “após a entrada em vigor… da *Online Safety Act*… a redução no número de usuários… foi acompanhada por um aumento expressivo na busca por serviços de VPN”. A Strima corrobora com dados específicos: “o provedor suíço Proton VPN relatou um aumento de 1.800% nos cadastros… indicando que milhares de usuários — inclusive menores — recorrem ao uso de redes privadas virtuais”.

A Associação Brasileira de Anunciantes (ABA) enquadra essa evasão como um risco aumentado, argumentando que a regulação pode "*encourage users to relocate to less restrictive jurisdictions… exposing users… to heightened risks*". Instituto Alana traz dados técnicos sobre a sofisticação da burla, revelando que "menores estão utilizando métodos cada vez mais sofisticados… com VPNs e '*deep-fakes'* ou 'selfies' geradas por IA representando 33% e 11% dos casos". Ela destaca que o método mais comum (38%) é analógico: "uso de documentos… emprestados ou comprados de adultos". A BRASSCOM sintetiza a limitação inerente da tecnologia, afirmando que "processos excessivamente complexos… tendem a desestimular o uso legítimo… e incentivar fraudes", sugerindo que a rigidez gera a própria evasão que busca combater.

3.7.4 Terminologia e conceitos-chave

O vocabulário dos participantes revela que os riscos são semanticamente construído não como uma falha técnica pontual, mas como a instauração de uma arquitetura de "vigilância" e "perfilamento", onde a infraestrutura de proteção é descrita através de termos que denotam perigo iminente, como "honeypots", "pontos únicos de falha" e "alvos de alto valor".

O campo semântico da segurança é dominado pelo medo da centralização, descrita pelos participantes através da metáfora técnica nativa do "*honeypot*" (ou "pote de mel"). A Zetta, o Instituto Alana e a Internet Society utilizam este termo exato para descrever a inevitabilidade do ataque a bases de dados centralizadas. O léxico aqui é militarizado e fatalista: fala-se em "superfície de ataque", "alvos prioritários" e "vazamentos massivos". A Strima e a DiraCom expandem esse vocabulário para a esfera política, substituindo "proteção" por "vigilância estatal" e "controle social". O termo "dissidentes" é introduzido pela Strima para qualificar o risco de perseguição por "governos autoritários", enquanto a Zetta utiliza o adjetivo jurídico "inconstitucional" para descrever o monitoramento da atividade dos cidadãos. A Coalizão Direitos na Rede e o CGI.br empregam a expressão "registros de navegação" associados à "identidade civil" para definir o mecanismo exato da quebra de anonimato, rejeitando a formação de um histórico perene do comportamento online.

No âmbito da economia dos dados, o léxico transita da “segurança” para a “extração”. O termo nativo central é “perfilamento” (*profiling*). O Instituto Alana e uma contribuinte acadêmica utilizam repetidamente termos como “uso secundário”, “enriquecimento de perfil” e “finalidades diversas” para descrever o desvio de função dos dados coletados. A PROTESTE introduz o conceito de “grafo social” para ilustrar o resultado do cruzamento de informações, enquanto a AMOBITEC alerta para a “inferência de dados comportamentais”. Uma terminologia específica emerge em relação à Inteligência Artificial: a eSapiens e a Family Talks falam em “treinamento de modelos proprietários” e “refinamento de tecnologias”, denunciando o uso da biometria infantil não para verificar, mas para “alimentar bases” de algoritmos generativos sem consentimento.

A discussão sobre o anonimato mobiliza um vocabulário técnico de desanonimização. A Microsoft e a Strimautilizam os termos “reidentificação” e “vinculação indireta” para descrever como “metadados técnicos” podem ser usados para rastrear indivíduos. Uma contribuinte acadêmica refina esse léxico ao incluir a dimensão doméstica, falando em “inferências sobre a estrutura familiar”. Em resposta a essa fragilidade, o Alana introduz o léxico da padronização técnica, citando a norma “ISO/IEC 27556” e o conceito de “*Privacy Enhancing Data De-identification Framework*” como vocabulário de solução.

Finalmente, a ineficácia da medida é descrita através de um léxico de evasão e substituição. O termo “VPN”(Rede Privada Virtual) é onipresente nas falas da eSapiens, Strima e Alana, que o associam a uma “migração” para “ambientes menos seguros”. A Associação Brasileira de Anunciantes (ABA)utiliza a expressão *“relocate to less restrictive jurisdictions*” (realocar-se para jurisdições menos restritivas) para descrever a fuga geográfica digital. A fraude técnica é descrita com neologismos contemporâneos como *“deep-fakes*” e “selfies geradas por IA”, indicando que o vocabulário da burla evoluiu da simples mentira para a falsificação sintética de identidade.

A Figura 6 representa um Mapa Semântico de Riscos e Ameaças, desenhado para representar a topografia do medo e da vulnerabilidade conforme expressa pelo vocabulário nativo dos participantes na categoria RISCOS ESPECÍFICOS (RISC).

Figura 6: Síntese da divisão do discurso sobre riscos

Fonte: produção própria

Este grafo espacializa os cinco grandes vetores de ameaça identificados, conectando os conceitos abstratos às suas manifestações técnicas e sociais específicas:

1. **Polo: Arquitetura da Vigilância (Vermelho - Topo)**

- Lógica: Representa o medo do Estado e do controle social.
- Vocabulário: O léxico aqui é constitucional e político. Termos como “Vigilância” e “Aparato de Controle” denunciam a escala do problema. A conexão com “Rastreamento de Dissidentes” e “Identidade Civil” ilustra o temor de que a verificação de idade se torne uma ferramenta de perseguição política, sendo qualificada juridicamente como “Inconstitucional”.

2. **Polo: Vulnerabilidade Técnica (Laranja - Centro)**

- Lógica: O coração técnico do problema: a centralização inevitável.
- Vocabulário: Dominado pela metáfora nativa do “*Honeypot*”. Este cluster conecta a causa (“Centralização de Dados”) à consequência (“Vazamentos Massivos”), explicando que a criação de bases valiosas gera “Alvos de Alto Valor” e “Pontos Únicos de Falha”, exacerbados por uma “Infraestrutura Inadequada” das empresas.

3. **Polo: Economia Extrativista (Turquesa - Direita)**

- Lógica: O desvio de finalidade para lucro e desenvolvimento tecnológico.
- Vocabulário: Foca na exploração dos dados. O termo central é “Perfilamento” (*Profiling*). A análise revela um léxico moderno de exploração: “Treinamento de IA” e “Alimentar Bases de Algoritmos” aparecem como novas formas de extração de valor da biometria infantil, configurando um “Uso Secundário” não autorizado.

4. **Polo: Erosão do Anonimato (Azul Claro - Esquerda)**

- Lógica: A morte da privacidade através da inferência.
- Vocabulário: Descreve a mecânica sutil da desanonimização. Não é apenas saber o nome, é a “Reidentificação” através de “Metadados Técnicos”. O termo “Inferência Familiar” destaca o risco de devassar a vida doméstica através do cruzamento de dados, culminando no “Fim do Anonimato”.

5. **Polo: Reação & Burle (Cinza - Base)**

- Lógica: A resposta do usuário à arquitetura de controle.
- Vocabulário: O léxico da evasão. “Uso de VPNs” e “Jurisdições Menos Restritivas” descrevem a fuga geográfica. A sofisticação tecnológica da fraude é capturada pelos termos “*Deep-fakes*” e “Selfies Geradas por IA”, indicando que a barreira técnica estimula o desenvolvimento de contramedidas pelos próprios usuários (inclusive crianças).

Esta visualização demonstra que, para os participantes, o “Risco” não é uma eventualidade, mas uma estrutura composta: uma arquitetura centralizada (*Honeypot*) que alimenta a vigilância (Estado) e a extração econômica (Mercado), gerando como resposta a evasão (VPNs).

Quadro Comparativo: Posições sobre Riscos específicos (RISC)

DIMENSÃO DE ANÁLISE	SETOR PRIVADO (Plataformas, Associações e Advocacia)	SOCIEDADE CIVIL E ACADEMIA	POSIÇÕES INTERMEDIÁRIAS OU DIVERGENTES
Vigilância Estatal e Controle Social	**Preocupações constitucionais:** Argumentos de que obrigações de coleta massiva podem ser questionadas à luz de direitos civis e liberdades fundamentais. Preocupação com a criação de bases de dados que possam ser requisitadas por governos.	**Preocupações com direitos fundamentais:** Argumentos baseados na privacidade e liberdade de expressão. Foco em impedir a criação de registros de navegação e identidade civil que permitam monitoramento de jovens e dissidentes.	**Convergência transversal:** Contribuintes de diferentes setores manifestaram preocupações com vigilância, unindo argumentos de liberdades econômicas e de direitos humanos contra infraestruturas centralizadas de identificação.
Mineração Comercial e Treinamento de IA	**Limitação de escopo:** Argumentos para restringir proibições ao uso de dados para publicidade direcionada a crianças especificamente, mantendo possibilidade de uso para aprimoramento de produtos.	**Vedação ampla de uso secundário:** Argumentos favoráveis à vedação total de uso secundário de dados de verificação. Dados de segurança devem ser isolados de bases de marketing. Oposição ao uso de biometria infantil para treinamento de IA.	**Posição cautelosa no setor privado:** Algumas associações setoriais adotaram postura mais restritiva que a média do setor, alertando contra coleta desproporcional e manifestando preocupação com riscos de compliance.
Centralização de Dados e Honeypots	**Risco associado à obrigação:** Argumentos de que a obrigação de verificar criará bases de dados centralizadas que se tornam alvos de ataques. Preocupação com responsabilização por vazamentos decorrentes de exigência regulatória.	**Risco associado à arquitetura:** Argumentos de que a centralização cria ponto único de falha. Preocupação com a capacidade técnica de empresas (especialmente menores) de proteger dados sensíveis.	**Defesa de centralização governamental:** Algumas plataformas defenderam que a verificação seja centralizada no Governo, argumentando que o Estado teria maior capacidade de custódia segura de dados sensíveis.

DIMENSÃO DE ANÁLISE	SETOR PRIVADO (Plataformas, Associações e Advocacia)	SOCIEDADE CIVIL E ACADEMIA	POSIÇÕES INTERMEDIÁRIAS OU DIVERGENTES
Eficácia, Evasão e Fraude	**Evasão como externalidade:** Argumentos de que a regulação pode gerar migração de usuários para ambientes não regulados, com dados sobre aumento de VPNs em jurisdições com verificação obrigatória.	**Evasão técnica:** Argumentos de que a tecnologia é vulnerável a técnicas de engenharia social (*deepfakes*, documentos falsos). A preocupação é com a facilidade de evasão por usuários com conhecimento técnico.	—
Privacidade Doméstica	**Foco no usuário direto:** A preocupação com privacidade concentra-se no dado do usuário verificado (criança ou adulto).	**Foco no núcleo familiar:** Argumentos de que a verificação pode revelar informações sobre a estrutura familiar através do cruzamento de dados, afetando a privacidade de terceiros não verificados.	—

3.8 Eixo 8: Impactos e Barreiras (IMPACT)

3.8.1 Visão geral e definição do eixo

O eixo IMPACTOS E BARREIRAS (CAT_IMPACT) agrupa os argumentos sobre as externalidades operacionais, econômicas e sociais decorrentes da implementação da verificação de idade, destacando o risco de exclusão digital de populações vulneráveis devido às limitações de *hardware*, conectividade e documentação , bem como a ineficácia de modelos baseados em consentimento parental diante da baixa literacia digital e diante dos diferentes níveis de competência digital das famílias. Os atores apontam que os custos de conformidade tendem a gerar assimetrias de mercado que penalizam pequenas e médias empresas em favor de grandes plataformas consolidadas , além de preverem o repasse financeiro ao consumidor final e a degradação da experiência de uso (fricção). As unidades de conteúdo também descrevem barreiras à fiscalização estatal causadas pela opacidade das arquiteturas corporativas e fragmentação institucional , alertam para a violação da autonomia progressiva de adolescentes entre 16 e 18 anos e indicam a probabilidade de

migração de usuários para ambientes não regulados ou para o uso de ferramentas de evasão técnica como VPNs.

3.8.2 Frequência e relevância dos temas

A distribuição de frequência do eixo Impacto e Barreiras (IMPACT) aponta para uma preponderância das preocupações com as externalidades sociais e as capacidades institucionais de aplicação da norma, com o código *IMPACT_EXCLUSAO_DIG* (9) ocupando a posição de maior recorrência, focado nos riscos de restrição de acesso a populações vulneráveis. Em sequência, o código *IMPACT_FISCALIZ* (8) agrupa os desafios práticos de auditoria e *enforcement*, enquanto a eficácia das medidas dependente da competência técnica dos responsáveis é abordada em *IMPACT_LITERACIA_FAMILIAR* (6). Um bloco intermediário de relevância, com 4 ocorrências para cada código, reúne as implicações econômicas e operacionais — *IMPACT_BARREIRA_PME*, *IMPACT_CUSTO_CONS* e *IMPACT_FRICCAO_USUARIO* — tratando, respectivamente, da viabilidade para pequenas empresas, do repasse financeiro ao consumidor e da degradação da experiência de navegação. A base da distribuição, composta pelos códigos *IMPACT_AUTONOMIA_JUVENIL* e *IMPACT_MERCADO_PARALELO* (3 unidades cada), registra os argumentos sobre violações de direitos progressivos de adolescentes e o potencial deslocamento de usuários para ambientes digitais não regulados.

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
IMPACT_EXCLUSAO_DIG	9	Preocupações com exclusão digital de populações vulneráveis ou sem documentação formal.
IMPACT_FISCALIZ	8	Discussões sobre desafios práticos de fiscalização, auditoria e barreiras institucionais para aplicação da norma.
IMPACT_LITERACIA_FAMILIAR	6	Preocupações com eficácia limitada em razão da falta de competência técnica dos pais ou responsáveis para configurar ferramentas de controle.
IMPACT_BARREIRA_PME	4	Preocupações com custos de conformidade que podem representar barreira significativa para pequenas e médias empresas.
IMPACT_CUSTO_CONS	4	Preocupações com repasse dos custos da verificação ao consumidor final.

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
IMPACT_FRICCAO_USUARIO	4	Preocupações com impacto na experiência do usuário, incluindo lentidão e abandono do serviço.
IMPACT_AUTONOMIA_JUVENIL	3	Preocupações com impacto sobre a autonomia progressiva e a privacidade de adolescentes (16-17 anos).
IMPACT_MERCADO_PARALELO	3	Preocupações com migração de usuários para plataformas não reguladas ou de origem não identificada.
TOTAL	**41**	

3.8.3 Principais Argumentos

A. Barreira para PMEs

Este código captura o temor de que a regulação consolide monopólios ao inviabilizar pequenos competidores. A Samsung alerta que “exigir soluções complexas ou de alto custo de PMEs seria desproporcional e poderia gerar efeitos anticompetitivos”, defendendo “prazos razoáveis e estímulos à adequação progressiva”. A BRASSCOM corrobora que a “infraestrutura complexa” pode ser “inviável para muitas empresas”, sugerindo uma regulação baseada em princípios e não em métodos prescritivos.

A Claro S.A. propõe uma saída arquitetural para mitigar esse impacto: permitir que serviços optem por apenas uma camada de verificação (loja ou app) quando suficiente, pois isso “reduz custos e complexidades técnicas”. Em contrapartida, a Meta argumentou que sua solução centralizada reduziria barreiras para desenvolvedores menores, que não precisariam criar sistemas próprios de verificação.

B. Exclusão digital

A fenomenologia da exclusão digital não é tratada aqui como um inconveniente técnico, mas como uma violação de direitos fundamentais. Há um consenso transversal de que a rigidez técnica punirá desproporcionalmente os vulneráveis. O CGI.br inaugura a crítica ao identificar o “risco de exclusão digital de crianças e adolescentes cujos responsáveis não possuem acesso digital”, estendendo a preocupação a “famílias em vulnerabilidade social, migrantes ou crianças e adolescentes em acolhimento institucional”. Esta perspectiva é corroborada

pela PROTESTE, que adota um tom normativo ao afirmar que “é essencial que a estrutura regulatória não crie barreiras de acesso”, alertando que soluções complexas violam o “espírito do Estatuto Digital” ao ampliar desigualdades.

A materialidade da exclusão é detalhada pelo Instituto Alana, que desloca o debate para o hardware, notando que “dispositivos com câmeras mais antigas ou de baixa qualidade podem ter taxas de erro maiores”, criando uma discriminação baseada na “qualidade do hardware do usuário”. A Federação do Comércio de SP adiciona a camada educacional, argumentando que o “alto índice de analfabetismo funcional” no Brasil transforma métodos sofisticados em “barreiras intransponíveis”.

A Electronic Frontier Foundation (EFF) introduz uma dimensão crítica de direitos humanos, questionando “como garantir que os métodos de verificação de idade não resultem na exclusão digital de jovens marginalizados ou sem documentação”, e alertando que a medida pode “restringir o acesso de crianças e adolescentes a recursos online para procurar cuidados, educação ou assistência”. Um contribuinte da sociedade civil adota uma postura fatalista sobre a segurança técnica, respondendo que “não é possível assegurar isso considerando a volatilidade desses próprios serviços”. Uma contribuinte acadêmica sintetiza a visão acadêmica ao reiterar o risco para aqueles com “menor acesso a dispositivos, conexão ou documentação regular”.

C. Custo ao consumidor

A discussão sobre custos não é abstrata. A eSapiens oferece a análise mais detalhada, quantificando o impacto financeiro: “uma validação simples via API Cadastral… custaria entre R0,39…eR3,50 por validação individual”. O ator conclui que para um site com “50 milhões de acessos mensais”, esse custo seria “impraticável” e tornaria a operação “insustentável, levando ao encerramento das atividades”.

A Zetta e a Câmara Brasileira da Economia Digital (camara-e.net) utilizam o argumento do custo para defender a flexibilidade, afirmando que “mecanismos excessivamente rígidos podem elevar custos” e que a “padronização excessiva pode favorecer alguns sistemas proprietários… aumentando custos para todo o ecossistema”. O Instituto Alana, focando no direito do consumidor, estabelece a premissa de que “deve-se garantir a gratuidade para o usuário final”, impedindo que a segurança se torne um produto de luxo.

D. Literacia familiar insuficiente

A narrativa central aqui é a insuficiência do "consentimento parental" em um país com baixo letramento digital. O Instituto Alana é enfático ao declarar que "sistemas que dependem dos pais… falham quando os próprios pais não possuem competência técnica", apontando a "disparidade na literacia digital" como um fator de desigualdade que afeta o uso de infraestruturas como o "GOV.br". A Coalizão Direitos na Rede diagnostica uma "baixa cultura de segurança digital", onde famílias "compartilham senhas ou dispositivos sem restrições".

A Federação do Comércio de SP reitera o impacto do "analfabetismo funcional", enquanto a PROTESTE exige "transparência ativa", argumentando que "pais, muitas vezes, não compreendem os riscos ou como funcionam os sistemas". A ABINEE traz uma crítica específica à materialidade da informação, argumentando que a exigência legal de adesivos em embalagens "não representa a forma mais eficaz", pois a embalagem é "descartada logo após o primeiro uso", defendendo "alternativas digitais" como QR Codes nas telas iniciais.

E. Fricção e usabilidade

A "fricção" é descrita como o inimigo da usabilidade e do acesso legítimo. O CGI.br adverte que a implementação "não deve inviabilizar o uso da internet ou criar fricção excessiva que degrade a experiencia do usuário". O Instituto Alana alinha-se pragmaticamente a essa visão de UX, notando que é "necessário equilibrar a robustez… para evitar que o processo de verificação leve ao abandono do serviço legítimo".

A Câmara Brasileira da Economia Digital (camara-e.net) e a Zetta reiteram que "exigências rígidas e descontextualizadas podem limitar o acesso legítimo", utilizando o termo "fricção" como sinônimo de falha de design regulatório que pode "comprometer a inovação".

F. Mercado paralelo e autonomia juvenil

O risco de que a regulação fomente a ilegalidade é central neste argumento. A Associação Brasileira de Anunciantes (ABA) utiliza o termo "obrigatoriedade da verificação de idade" para alertar que isso pode "incentivar os usuários a migrarem para jurisdições menos restritivas… expondo-os… a riscos maiores". A eSapiens detalha o mecanismo de evasão, prevendo a migração para a "*dark web* ou serviços sediados em paraísos digitais" e o estímulo ao uso de "ferramentas como VPNs". A Câmara Brasileira da Economia Digital (camara-e.net) concorda que o rigor excessivo pode "incentivar práticas informais", derrotando o propósito protetivo da norma.

Há, ainda, uma nuance jurídica e pedagógica sobre os direitos dos adolescentes mais velhos. A Samsung articula a defesa da "autonomia progressiva", argumentando que adolescentes entre 16 e 18 anos, que "podem, inclusive, votar", possuem "maior autonomia de decisão". O ator defende que a aferição não deve ser "meramente restritiva", mas possibilitar o acesso a conteúdos adequados "sem necessariamente precisar de autorização do pai". A Câmara Brasileira da Economia Digital (camara-e.net) apoia essa visão, pleiteando um arcabouço que "respeite a autonomia das famílias" e permita escolhas proporcionais.

G. Desafios de fiscalização

Este argumento revela a descrença na capacidade estatal de fiscalização e a resistência à opacidade corporativa. A Family Talks condiciona a eficácia da lei à ação estatal, afirmando que "sem os quais a lei torna-se letra morta", exigindo auditoria de tecnologias para assegurar a "anonimização". No entanto, a Strima aponta a fragmentação institucional como obstáculo, citando a necessidade de evitar "conflitos de competência entre órgãos fiscalizadores (ANPD, Senacon, Ministério da Justiça)" e alertando contra "zonas cinzentas de conformidade".

O Instituto Alana aponta a lógica econômica das plataformas, argumentando que elas "frequentemente não têm incentivo econômico para evitar a coleta de dados adicionais", pois a identificação "alimenta seus modelos de negócio". O Instituto também traz evidências do *Australia Age Assurance Trial* para alertar que uma minoria de provedores retém dados "sob pretexto de 'preparação para demandas

investigatórias'". A Coalizão Direitos na Rede reforça a crítica à "pouca transparência das plataformas sobre seus algoritmos", o que dificulta a "responsabilização por falhas".

Do lado do setor privado, uma contribuinte acadêmica relata que as empresas temem a "insegurança jurídica e multas desproporcionais", demandando "diretrizes normativas claras e uniformes" para evitar a fragmentação. A PROTESTE identifica uma lacuna crítica na cadeia de valor: os "aplicativos pré-instalados" que não passam pelas lojas oficiais, operando fora do "fluxo regulável", o que "compromete a coerência do sistema".

3.8.4 Terminologia e conceitos-chave

Esta análise transversal do léxico mobilizado pelos participantes investiga a terminologia nativa utilizada para descrever as externalidades negativas e os obstáculos práticos à implementação da verificação de idade. O vocabulário in vivo revela que o fenômeno não é tratado apenas como um desafio técnico, mas como um vetor de "exclusão" e "fricção", onde a desigualdade material e cognitiva do usuário brasileiro é o ponto central da argumentação. A "exclusão digital" é o termo estruturante, mas os participantes o refinam com uma gramática da materialidade: o Instituto Alana e a PROTESTE descrevem a barreira não apenas pela falta de acesso, mas pela "qualidade do hardware", citando especificamente "dispositivos com câmeras mais antigas" e de "baixa resolução" que geram "taxas de erro maiores". A exclusão é, portanto, descrita através do léxico da obsolescência tecnológica, que penaliza quem não possui "dispositivos modernos". Paralelamente, a barreira cognitiva é articulada através dos termos "analfabetismo funcional" e "literacia digital". A Federação do Comércio de SP e a Coalizão Direitos na Rede utilizam esses conceitos para qualificar a "competência técnica" das famílias como insuficiente, transformando o "consentimento parental" em uma ficção jurídica diante da incapacidade real de operar as ferramentas.

No campo semântico econômico e operacional, o termo nativo dominante é a "fricção". Utilizado repetidamente pelo setor privado (Zetta, CGI.br, Camara-e.net), este vocabulário descreve a degradação da "experiência do usuário" que leva ao "abandono do serviço". A fricção não é apenas um incômodo, mas um custo

quantificável que torna a operação “insustentável”. A eSapiens introduz um léxico contábil preciso para descrever esse fenômeno, citando valores de “R$0,39” a “R$3,50” por validação, argumentando que tal custo geraria o “encerramento das atividades”. A assimetria de mercado é descrita através de termos como “efeitos anticompetitivos” e “barreiras de entrada”, onde a Samsung e a BRASSCOM alertam que a exigência de “infraestrutura complexa” favorece a concentração de mercado, uma vez que penaliza desproporcionalmente as “PMEs” (Pequenas e Médias Empresas). A Meta, apropriando-se desse léxico, oferece sua solução centralizada como forma de diminuir essas “barreiras”, consolidando uma narrativa de dependência tecnológica.

A ineficácia da norma e a reação do usuário são descritas através de um vocabulário de evasão e falência institucional. A Family Talks utiliza a expressão “letra morta” para descrever uma lei sem capacidade de enforcement. A evasão do usuário não é descrita como crime, mas como uma migração racional para o “mercado paralelo” ou para “paraísos digitais”. A Associação Brasileira de Anunciantes (ABA) e a eSapiens empregam termos como “*dark web*”, “VPNs” e “ferramentas de evasão” para caracterizar o efeito de a medida protetiva que empurrar o sujeito para o risco não regulado. A fiscalização estatal é descrita através do léxico da opacidade e da confusão: “zonas cinzentas”, “conflitos de competência” e “ausência de monitoramento proativo” compõem o cenário descrito pelo Instituto Alana e pela Strima, onde a falta de transparência algorítmica impede a “responsabilização”.

Finalmente, o espectro de sentidos incorpora uma terminologia de direitos civis emergentes, focada na “autonomia progressiva”. A Samsung e a Câmara Brasileira da Economia Digital utilizam este termo jurídico para contestar a visão da verificação como um instrumento “meramente restritivo”. O vocabulário aqui foca na capacidade civil de adolescentes entre 16 e 18 anos, mobilizando termos como “direito de acesso”, “capacidade civil relativa” e a prerrogativa de “votar” para argumentar contra a exigência de “autorização do pai”. A Electronic Frontier Foundation (EFF) complementa esse léxico ao associar a verificação à perda de “anonimato”, descrevendo a identificação obrigatória como uma barreira para a busca de “cuidados” e “educação”, situando a privacidade não como ocultação, mas como condição para o exercício de direitos por populações marginalizadas.

A Figura 7 representa um Diagrama de Polos e Vocabulário In Vivo, rigorosamente corrigida para refletir apenas os termos validados na análise textual da categoria IMPACTOS E BARREIRAS (CAT_IMPACT).

Figura 7: Síntese dos temas em cada polo dos discursos sobre impactos e barreiras

Fonte: produção própria

Este diagrama espacializa os quatro vetores de resistência identificados, destacando a terminologia utilizada para descrever cada dimensão do problema. Esta visualização demonstra que os “Impactos” não são eventos isolados, mas sistemas de linguagem que conectam a falha técnica (Vermelho) e institucional (Azul) à inviabilidade econômica (Turquesa) e, finalmente, à evasão da norma (Laranja).

Quadro Comparativo: Posições sobre Impactos e barreiras (IMPACT)

DIMENSÃO DE ANÁLISE	SETOR PRIVADO	SOCIEDADE CIVIL E ACADEMIA	POSIÇÕES INTERMEDIÁRIAS OU CONVERGENTES
Natureza da Barreira	**Barreira econômica e operacional:** Foco no custo de implementação e na sustentabilidade do negócio. Argumentos de que custos de verificação (citados valores entre R$0,39 e R$3,50 por validação) podem inviabilizar a operação de sites de alto tráfego.	**Barreira material e cognitiva:** Foco na desigualdade estrutural. A barreira é física (acesso a dispositivos com câmeras de qualidade) e educacional (capacidade de operar sistemas complexos). Argumentos de que a exclusão decorre de falhas de design, não de escolha do usuário.	**Convergência sobre literacia:** Contribuintes de diferentes setores convergiram no diagnóstico de que a complexidade técnica representa barreira tanto de consumo quanto de cidadania.
Impacto na Estrutura de Mercado	**Assimetria competitiva:** Argumentos de que exigências complexas criam barreiras de entrada para pequenas e médias empresas, favorecendo a concentração de mercado em grandes plataformas que já possuem infraestrutura.	**Exclusão de populações vulneráveis:** Foco no impacto sobre o cidadão. Argumentos de que a exigência de tecnologia de ponta cria barreira de acesso, onde apenas quem possui documentos regularizados e dispositivos modernos consegue exercer direitos digitais.	**Soluções centralizadas como alternativa:** Algumas plataformas propuseram soluções de verificação centralizada como forma de reduzir custos para desenvolvedores menores, embora isso gere debates sobre dependência de infraestrutura.
Governança e Fiscalização	**Preocupações com segurança jurídica:** A ausência de fiscalização clara é apontada como risco para as empresas. Contribuintes citam a falta de clareza normativa e o conflito de competência entre órgãos estatais como geradores de incerteza e risco de compliance.	**Preocupações com efetividade:** A ausência de fiscalização é apontada como obstáculo à proteção efetiva. Contribuintes citam a falta de monitoramento proativo e a opacidade dos algoritmos como impedimentos para que o Estado verifique a proteção real das crianças.	—
Direitos e Autonomia do Usuário	**Experiência do usuário:** A autonomia é abordada sob a ótica do consumidor. Argumentos de que barreiras rígidas geram fricção excessiva, levando ao abandono do serviço legítimo.	**Direito ao acesso e anonimato:** A autonomia é abordada sob a ótica dos direitos humanos. Argumentos de que a identificação obrigatória impede jovens marginalizados de buscar	**Autonomia progressiva de adolescentes:** Alguns contribuintes do setor privado alinharam-se à defesa jurídica da autonomia progressiva de jovens de 16-18 anos, argumentando que essa

DIMENSÃO DE ANÁLISE	SETOR PRIVADO	SOCIEDADE CIVIL E ACADEMIA	POSIÇÕES INTERMEDIÁRIAS OU CONVERGENTES
		ajuda (saúde, educação) anonimamente.	faixa etária merece tratamento diferenciado.
Evasão e Consequências	**Migração para ambientes não regulados:** A evasão é vista como migração para jurisdições menos restritivas ou mercados informais. Argumentos de que a regulação pode prejudicar quem cumpre a norma e beneficiar quem opera fora dela.	**Exposição a riscos maiores:** A evasão é vista como falha do objetivo protetivo. Argumentos de que ao empurrar usuários para ambientes sem regulação, a norma pode expor crianças a riscos maiores do que os existentes nas plataformas reguladas.	—

3.9 Eixo 9: Desenho Regulatório e Governança (REGU)

3.9.1 Visão geral e definição do eixo

O Eixo DESENHO REGULATÓRIO (REGU) agrupa os argumentos sobre a arquitetura de governança digital. Enquanto contribuintes da sociedade civil apresentaram demandas por taxatividade (REGU_ORIENT_DEF) e auditoria pública (REGU_CERTIF_AUDITAB) como mecanismos de garantia de direitos e defesa de infraestrutura pública (REGU_API_ABERTA), contribuintes do setor privado enfatizaram a harmonização internacional (REGU_HARMONIZACAO) e a neutralidade tecnológica (REGU_NEUTRALIDADE) para garantir flexibilidade operacional. A convergência em torno do *Sandbox* (REGU_SANDBOX) atende a objetivos distintos conforme o setor: para uns, representa oportunidade de testar a proteção de direitos fundamentais; para outros, representa período de adequação gradual. A análise das demandas por prazos (REGU_PRAZOS) revela preocupações tanto com segurança jurídica quanto com a efetividade da proteção.

3.9.2 Frequência e relevância dos temas

A distribuição de frequência da categoria Desenho Regulatório (REGU) evidencia uma preponderância do código REGU_ORIENT_DEF (82), que concentra quase metade das unidades da amostra (48,8%), indicando que a demanda principal dos participantes recai sobre a definição de conceitos, orientações e princípios

estruturantes antes da imposição de regras operacionais. Em um segundo estrato de relevância, observam-se as preocupações com a consistência sistêmica e a governança, representadas pelos códigos REGU_HARMONIZACAO (20) e REGU_CERTIF_AUDITAB (18), que buscam o alinhamento com marcos legais pré-existentes e a garantia de mecanismos de auditoria externa. As questões de implementação técnica e operacional compõem um bloco intermediário, abrangendo a defesa de interoperabilidade via REGU_API_ABERTA (14) e as objeções aos custos burocráticos e temporais expressas em REGU_COMPLEXIDADE (13) e REGU_PRAZOS (11). A base da distribuição é ocupada por propostas de flexibilidade tecnológica e experimentalismo, com os códigos REGU_NEUTRALIDADE e REGU_SANDBOX_registrando 5 ocorrências cada, sugerindo que a discussão sobre neutralidade de métodos e ambientes de teste é secundária frente à necessidade de clareza conceitual.

ANÁLISE DE SENSIBILIDADES — TABELA REGU (DEMANDAS REGULATÓRIAS)

CÓDIGO	FREQUÊNCIA	DESCRIÇÃO BREVE
REGU_ORIENT_DEF	82	Solicitações de definições claras, orientações ou princípios específicos por parte do regulador.
REGU_HARMONIZACAO	20	Argumentos sobre a necessidade de alinhamento com legislação nacional (LGPD) e marcos internacionais (GDPR, entre outros).
REGU_CERTIF_AUDITAB	18	Propostas de acreditação, auditoria ou certificação oficial de fornecedores de tecnologia de verificação.
REGU_API_ABERTA	14	Argumentos favoráveis a APIs abertas, interoperabilidade ou documentação pública de interfaces de verificação.
REGU_COMPLEXIDADE	13	Preocupações com burocracia, complexidade normativa ou insegurança jurídica decorrente da regulamentação.
REGU_PRAZOS	11	Solicitações de extensão de prazos, período de carência ou implementação gradual das obrigações.
REGU_NEUTRALIDADE	5	Argumentos de que a regulamentação não deve prescrever tecnologias específicas, mantendo neutralidade tecnológica.
REGU_SANDBOX	5	Propostas de ambientes de teste experimentais (*sandbox* regulatório) ou projetos-piloto.
TOTAL	**168**	

Note-se a alta prevalência de REGU_ORIENT_DEF (quase 50% dos dados), indicando uma forte demanda por clareza conceitual antes da implementação técnica.

3.9.3 Principais argumentos

A. Orientações e definições claras

A análise demonstra que não há consenso sobre o que significa “regular bem” nesse contexto. A PROTESTE articula uma defesa veemente de uma regulação baseada em princípios (“orientada a metas”), argumentando que “um marco orientado a princípios… tende a gerar resultados mais consistentes” do que regras rígidas que se tornam obsoletas. A Câmara Brasileira da Economia Digital (camara-e.net) alinha-se a essa visão, mas com um viés de mercado, alertando que “regulações excessivamente prescritivas tendem a gerar custos elevados… sem ganhos concretos”. O ponto de convergência aqui é a rejeição ao modelo “tamanho único” (*one-size-fits-all*).

A principal demanda regulatória não é por ausência de regras, mas por uma definição estrita que delimite o campo de responsabilidade. O CGI.br constrói o sentido da regulação como um mecanismo de contenção de danos, argumentando que a norma deve ser “enfática ao garantir e comprovar que a aferição etária seja utilizada estritamente de acordo com a LGPD, impedindo a proliferação de bases de dados indevidas”. Para este ator, a definição clara serve para barrar o “uso indiscriminado de biometria”. Em concordância, a eSapiens exige “requisitos regulatórios claros para o uso de biometria… associados a mecanismos robustos de fiscalização”, invocando a LGPD como o parâmetro de legitimidade que a ANPD deve fiscalizar.

Contribuintes do setor privado também demandaram definições claras, com ênfase na delimitação do escopo da lei a cenários de alto risco, argumentando pela necessidade de segurança jurídica e proporcionalidade. A Roku, por exemplo, argumenta que a regulamentação deve trazer “dispositivos expressos” que estabeleçam “a verificação como medida formal, restrita a contextos de alto risco”, rejeitando critérios uniformes. A Zetta reforça essa visão, alertando que se deve “evitar critérios subjetivos ou amplos que possam levar a verificações generalizadas e desproporcionais”.

A Coalizão Direitos na Rede e o Instituto Alana disputam o sentido desses princípios. Para eles, “princípios” não significam flexibilidade total, mas sim adesão estrita à “minimização de dados” e à “proteção integral” do ECA. O Alana introduz o conceito de “neutralidade do processo” como um princípio de design, onde a verificação deve ser invisível para quem verifica (a plataforma não sabe quem é) e para quem é verificado (o usuário não sente fricção desnecessária). A Zetta tenta capturar o princípio da “proporcionalidade” para argumentar que pequenas empresas devem ter obrigações menores, transformando um princípio jurídico em uma estratégia de defesa comercial.

O Instituto Alana introduz uma disputa semântica fundamental dentro deste código, propondo a necessidade de “repensar o uso do vocabulário técnico”. O Alana argumenta que o termo “aferição etária” é hermético e “soa pouco acessível”, sugerindo a substituição por “prova de idade” ou “garantia de idade” para tornar a comunicação “mais clara e favorecer a compreensão pública”. Os objetivos da clareza normativa variam entre os contribuintes: enquanto o setor privado enfatizou a previsibilidade para conformidade regulatória, organizações da sociedade civil enfatizaram a transparência como instrumento de *accountability* pública.

B. Certificação e auditoria

A exigência de auditoria revela uma profunda desconfiança na autodeclaração das plataformas. O CGI.br estabelece que a “expectativa regulatória” é que operadores “demonstrem, e não apenas declarem, o atendimento à legislação”, recomendando “registros verificáveis” e “auditoria independente”. O termo chave é “demonstrar”. A Yoti traz um detalhamento técnico rigoroso para essa demonstração, indicando “auditores independentes, *hacking* ético, programas de recompensas” e certificação anual por terceiros acreditados. A Yoti não pede apenas regras, pede policiamento técnico_ (“penalidades claras para o não cumprimento”). O Instituto Alana vai além nessa demanda ao exigir “controle social”, argumentando que deve haver “transparência pública sobre relatórios de auditoria e painéis de desempenho, sujeitos ao escrutínio e controle da população”. Para a sociedade civil, a auditoria não é um processo burocrático interno, mas uma ferramenta política de responsabilização.

Uma contribuinte acadêmica propõe a institucionalização dessa confiança através da “criação de um selo ou certificação nacional de conformidade… com auditoria regulatória da ANPD”. O CTS-FGV expande essa ideia para um mercado regulado de confiança, sugerindo que “empresas privadas poderiam ser auditadas e certificadas pela Administração Pública”, criando um ecossistema de “verificação como Serviço (VaaS)”. O CTS-FGV sugere que o Estado atue como certificador, criando um mercado de “terceiros de confiança” auditados publicamente. O Match Group (Tinder) concorda com a auditoria, mas foca na “limitação estrita de finalidade”, exigindo que auditores verifiquem especificamente se os dados não estão sendo usados para lucro ou treino de IA. A Brasscom, contudo, silencia sobre auditorias obrigatórias, preferindo falar em “boas práticas”, sugerindo resistência a custos de compliance externo.

A Yoti, posicionando-se como fornecedora dessa confiança, defende que tecnologias de estimativa facial sejam aceitas “quando testados independentemente quanto à imparcialidade e resistência à falsificação”, transformando a auditoria em um requisito de entrada de mercado que favorece empresas especializadas em detrimento de soluções caseiras das plataformas.

C. *Sandbox* regulatório

O Sandbox Regulatório emerge como um ponto de convergência raro. O Instituto Alana defende a “Adoção progressiva e sandbox regulatório” para testar “métodos inovadores… antes da padronização obrigatória”. A Federação do Comércio de SP e a Coalizão Direitos na Rede convergem na defesa de “testes, pilotos e sandboxes” para experimentar soluções antes da obrigatoriedade geral. A BRASSCOM vê no sandbox uma forma de testar as famosas *Zero-Knowledge Proofs* sem o risco de inviabilizar o negócio (“favorece a experimentação responsável”). É a proposta de “aprender fazendo” em ambiente controlado, mitigando o risco de colapso sistêmico na implementação nacional.

Para a sociedade civil, o sandbox é um laboratório para testar a segurança e a privacidade (ver se o ZKP funciona); para a indústria, é um porto seguro (“*safe harbor*”) para desenvolver soluções “sem risco imediato de sanção”. Embora concordem com

o instrumento, seus objetivos finais divergem: uns querem provar a viabilidade da privacidade, outros querem provar a inviabilidade da rigidez.

D. APIs abertas

A discussão sobre APIs transcende a técnica e torna-se um debate sobre quem controla os trilhos da verificação. O Instituto Alana defende um modelo estatista de "Blind APIs e Integração Federada com Sistemas Públicos", onde o Estado disponibiliza "APIs de acesso cego a registros governamentais… mantendo a soberania nacional de dados". Essas APIs seriam conectadas a registros governamentais. A proposta é que o Estado disponibilize infraestrutura para que empresas verifiquem atributos (ex.: "está matriculado na escola?") sem ver o dado bruto. Isso é descrito como forma de manter a "soberania nacional de dados". A FNPETI reforça essa visão sob a ótica da inclusão econômica, argumentando ser "crucial pensar em soluções públicas, gratuitas… preferencialmente por meio de APIs públicas", para permitir que pequenos desenvolvedores e projetos de software livre sobrevivam.

Em contraste, grandes empresas propõem infraestruturas proprietárias ou controladas pelo sistema operacional. A Apple promove sua "*Declared Age Range API*", enquadrando-a como uma ferramenta em que "os pais podem permitir que seus filhos compartilhem a faixa etária". A Meta descreve a "API de Idade" como uma "interface a nível de sistema que fornece automaticamente a faixa etária", argumentando que isso "garante que terceiros não estejam envolvidos no processo". Há aqui uma disputa de arquitetura: a sociedade civil quer APIs públicas para garantir soberania e custo zero; as plataformas querem APIs de sistema (OS) para manter o controle do ecossistema e evitar a fricção de verificadores externos.

A Associação Brasileira de Anunciantes (ABA) tenta mediar esse conflito propondo "padrões interoperáveis" e "componentes públicos, modulares" para evitar a dependência de um único fornecedor, alinhando-se parcialmente à visão de infraestrutura pública da FNPETI, defendendo "soluções públicas, gratuitas… e de código aberto" para incluir pequenos desenvolvedores. O argumento é econômico e social: se a verificação for cara e proprietária, apenas grandes players sobreviverão. A Meta e a Apple tentam capturar essa demanda apresentando suas próprias APIs

(*Declared Age Range API, Play Age Signals*) como a solução padrão de mercado que já resolve o problema.

E. Harmonização normativa

A harmonização internacional é construída pelos atores como uma espécie de selo de validação técnica e política. A Yoti, interessada em exportar seu modelo de negócio, satura o discurso com referências ao Reino Unido e Austrália, citando que a "Força-Tarefa Australiana de Tecnologia de Garantia de Idade concluiu que a estimativa da idade facial atingiu a maturidade técnica". A empresa argumenta que reguladores como o ICO e Ofcom "reconhecem a predição de idade como um método… válido e 'altamente eficaz'", tentando naturalizar no Brasil o consenso técnico que alega existir na Europa. A Meta adere a essa estratégia de legitimação externa, afirmando que "Reguladores como o ICO e Ofcom do Reino Unido reconhecem a predição de idade" como forma de validar seu uso de IA para classificação de adultos.

A Claro S.A. e a Federação do Comércio de SP (Fecomercio) utilizam a harmonização para defender a flexibilidade. A Claro cita *a 5Rights Foundation* e a *Data Protection Commission* (DPC) da Irlanda para sustentar que "a proporcionalidade é o eixo central" e que "não há modelo único aplicável". A Fecomercio invoca o modelo europeu "*EUConsent*" e o "*Blueprint for Age Verification Solution*" para defender uma arquitetura "descentralizada e *open source*", contrapondo-se indiretamente aos modelos proprietários das grandes empresas.

O Instituto Alana utiliza a autoridade da CNIL francesa para legitimar suas propostas, argumentando que "considera-se proveitoso comparar os parâmetros internacionais… valorizando a síntese elaborada pela ANPD". A citação da CNIL serve como âncora de legitimidade: se a França faz, o Brasil tem respaldo para fazer. Ainda assim, o Instituto Alana traz a ressalva de soberania. Embora reconheça que "várias autoridades de regulação ao redor do mundo chegaram a resultados semelhantes", o instituto defende "valorizar a síntese elaborada pela ANPD, incorporando-lhe ajustes e aperfeiçoamentos", recusando uma transposição mecânica das normas estrangeiras e priorizando o fortalecimento da agência brasileira. A harmonização internacional é descrita como imperativo de sobrevivência econômica e técnica.

A PROTESTE e a BRASSCOM expandem esse argumento para a interoperabilidade de mercado. A BRASSCOM alerta que a fragmentação regulatória (regras brasileiras muito diferentes das globais) isolaria o país, encarecendo a operação de empresas multinacionais e dificultando a entrada de inovação. O Setor Privado via camara-e.net usa a harmonização como uma defesa, argumentando que o Brasil deve adotar padrões como *W3C Verifiable Credentials* e ISO/IEC 27566 para garantir que o sistema nacional converse com o mundo.

F. Prazos de implementação

A discussão temporal é pragmática. O Setor Privado (representado por Zetta, Camara-e.net) pede regimes de transição longos. O argumento não é de recusa, mas de viabilidade: "implementar verificações robustas exige tempo de engenharia". Pedem-se "janelas de adequação" e implementação escalonada (começar por grandes plataformas, depois médias). A Sociedade Civil tende a aceitar prazos razoáveis, desde que não virem procrastinação indefinida, focando mais na qualidade da solução final do que na pressa de uma implementação malfeita que gere vazamentos.

A Electronic Arts (EA) é extremamente prescritiva, solicitando um "prazo de cumprimento de doze meses após a emissão do decreto", argumentando que o prazo atual da lei (março de 2026) "*may be insufficient*". A Google reforça essa tática dilatória ao defender que a fiscalização "somente ocorra após a publicação de diretrizes finais e claras… e só considere a fiscalização após a publicação da orientação final". O setor privado constrói o argumento de que agir antes da regulação final da ANPD gera "insegurança jurídica" e "expectativas regulatórias inconsistentes".

A Federação do Comércio de SP propõe "modelos graduais e escalonados de implementação", sugerindo que a adequação não deve ser um evento único, mas um processo progressivo. A PROTESTE concorda com a necessidade de "períodos de transição adequados", mas alerta que isso não pode servir para a "adoção improvisada de soluções pouco confiáveis".

G. Crítica à complexidade

O setor privado apresentou argumentos de que a complexidade regulatória representaria risco à economia digital. A Zetta e a Câmara Brasileira da Economia Digital alertam que “modelos regulatórios uniformes… podem gerar custos desproporcionais, prejudicando a inovação e a própria concorrência”. A Kaspersky argumenta especificamente que “mandatos excessivamente prescritivos… podem criar barreiras, especialmente para startups”. Este argumento constrói a regulação rígida como inimiga da diversidade de mercado.

A Strima introduz um argumento consequencialista baseado em evidência empírica negativa, citando que “o provedor suíço Proton VPN relatou um aumento de 1.800% nos cadastros” após o Online Safety Act no Reino Unido. O ator usa esse dado para argumentar que a rigidez cria “um mercado paralelo de ‘VPNs infantis’”, tornando o sistema “ineficaz”. A complexidade, neste discurso, não gera proteção, mas evasão.

A Microsoft introduz uma crítica técnica ao modelo de “duas cancelas” (verificação no OS + verificação no App), argumentando que essa redundância não minimiza riscos, mas adiciona “fatores de risco” e complexidade desnecessária. O consenso no setor privado é que a complexidade regulatória é inimiga da segurança efetiva, pois empurra o usuário para a ilegalidade ou para plataformas não reguladas.

O Instituto Alana reconhece o problema do custo, mas propõe uma solução assimétrica: “os custos de conformidade não devem barrar o desenvolvimento… sendo necessária uma análise assimétrica e responsável”, defendendo gratuidade para o usuário e menores encargos para pequenos agentes, sem renunciar à exigência para os grandes.

G. Neutralidade tecnológica

A defesa da neutralidade tecnológica é defendida pelo Setor Privado como forma de evitar a obsolescência e o dirigismo estatal. A Federação do Comércio de SP argumenta que “somente por meio de abordagem… tecnicamente neutra será possível garantir… a competitividade”. A Electronic Arts solicita explicitamente “flexibilidade nos métodos de garantia de idade”, argumentando que permite uma

gama de opções seguras para que os mecanismos “permaneçam tecnologicamente neutros… e adaptáveis à inovação”. A Electronic Arts também reforça que regulações estáticas sobre métodos específicos (“métodos de garantia de idade excessivamente prescritivos…”) correm o risco de se tornarem obsoletas rapidamente. O princípio defendido é: o regulador define o resultado (não deixar criança entrar), a empresa define a tecnologia (como impedir). A BRASSCOM ecoa esse posicionamento, recomendando “fortemente que a regulamentação secundária brasileira não especifique métodos precisos”.

Este código funciona como uma vacina contra a imposição de soluções estatais (como o Gov.br obrigatório) ou biométricas caras. Contribuintes do setor privado sugerem manter o direito de escolher o método “mais adequado e pertinente ao contexto”, o que na prática significa manter a porta aberta para métodos de menor fricção (como inferência ou autodeclaração reforçada) em detrimento de verificações documentais rígidas.

3.9.4 Terminologia e conceitos-chave

O vocabulário *in vivo* organiza-se em torno de disputas semânticas sobre a natureza da obrigação, a fonte da autoridade e a viabilidade temporal da adequação.

No campo da definição normativa, observa-se uma tensão lexical entre termos de restrição e termos de ampliação do escopo regulatório. Atores do setor privado utilizam recorrentemente locuções como “dispositivos expressos” e “medida formal” para qualificar a verificação de idade, associando-as a termos restritivos como “contextos de alto risco”. Contribuintes do setor privado utilizaram termos como 'dispositivos expressos' e 'contextos de alto risco', argumentando contra 'critérios subjetivos ou amplos' que gerariam insegurança jurídica. Em contrapartida, órgãos gestores e acadêmicos mobilizam o léxico da “garantia” e da “comprovação”, exigindo que a norma seja “enfática”. O Instituto Alana introduz uma disputa terminológica direta ao propor a substituição do termo “aferição etária”, classificado como hermético, por “prova de idade” ou “garantia de idade”, buscando deslocar o sentido de um procedimento técnico para um direito assegurado.

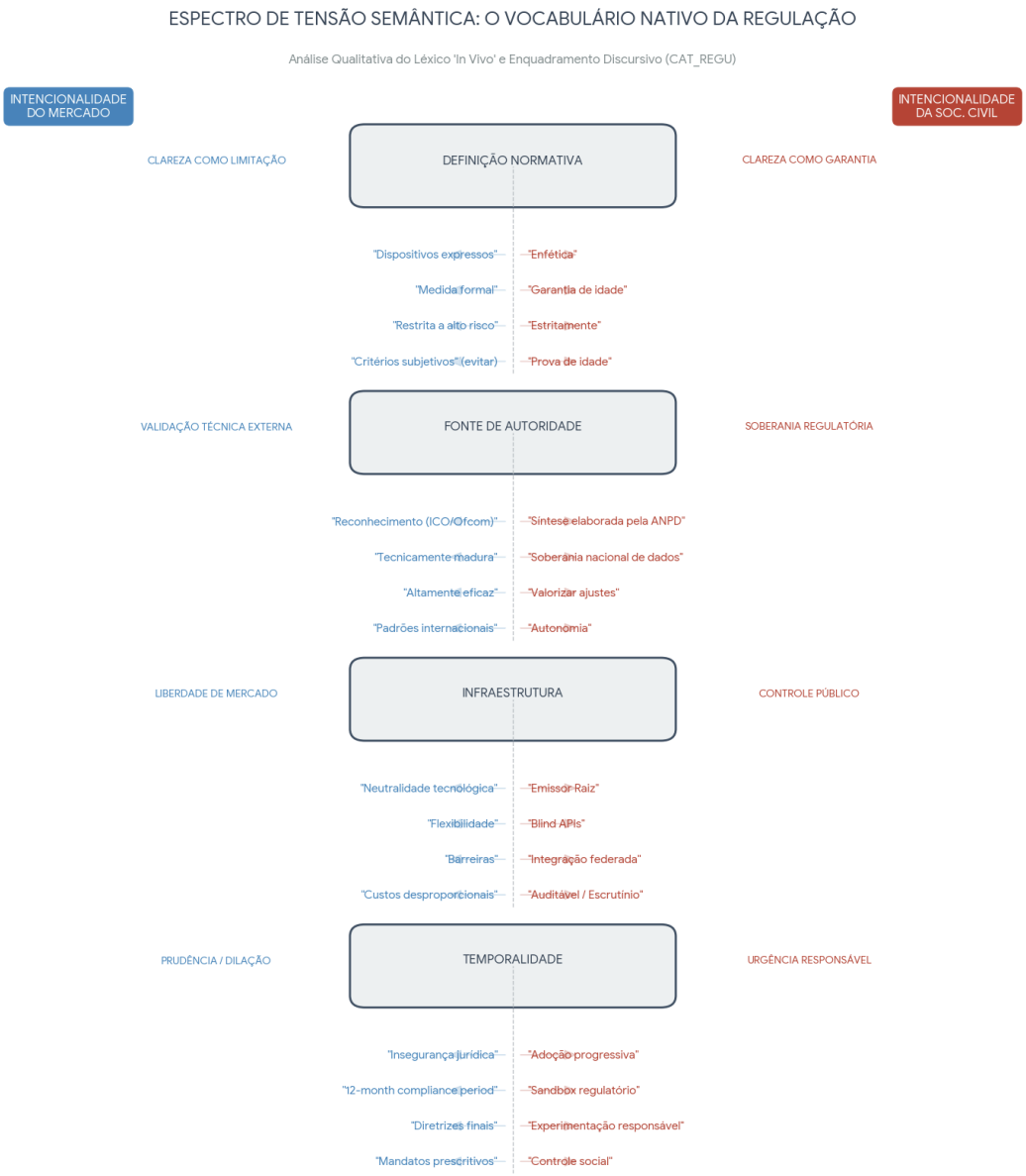
A autoridade regulatória é disputada através de um vocabulário de validação externa versus soberania interna. O léxico do setor privado apresenta referências a

entidades estrangeiras, citando “ICO”, “Ofcom” e “DPC da Irlanda” como fontes de “reconhecimento” e “validade”. O uso de termos como “tecnicamente madura” e “altamente eficaz” ao referir-se a normas do Reino Unido indica uma tentativa de naturalizar padrões externos. Por outro lado, o vocabulário da sociedade civil enfatiza a “síntese elaborada pela ANPD” e a “soberania nacional de dados”, utilizando termos como “valorizar” e “ajustes” para descrever a relação com normas internacionais, rejeitando a transposição automática. A infraestrutura é descrita por este grupo através de termos como “emissor raiz”, “integração federada” e “APIs de acesso cego”, enquanto o setor privado prefere a “neutralidade tecnológica” e a “flexibilidade”, associando a especificação técnica a “barreiras” e “custos desproporcionais”.

A temporalidade e a conformidade econômica geram um léxico específico de urgência e dilação. O setor privado emprega termos como “insegurança jurídica”, “expectativas inconsistentes” e “mandatos excessivamente prescritivos” para caracterizar a aplicação imediata da lei. A expressão “*twelve-month compliance period*” e a exigência de “diretrizes finais” funcionam como marcadores temporais que condicionam a ação à certeza absoluta. Em contraste, o vocabulário da sociedade civil foca no “controle social” e no “escrutínio”, ressignificando a transição não como espera, mas como período de “adoção progressiva”. O termo “*sandbox* regulatório” aparece como um ponto de convergência lexical, mas é descrito com finalidades distintas: para a indústria, é um espaço de “flexibilidades normativas” e “sem risco imediato de sanção”; para a academia e ativistas, é um *locus* de “experimentação responsável” para calibrar a proteção. O vocabulário in vivo desta categoria, portanto, transita entre a linguagem da imunidade jurídica (“*safe harbor*”, “barreiras”) e a linguagem da responsabilidade pública (“auditável”, “soberania”).

A Figura 8 apresenta a síntese dos temas em cada polo dos discursos sobre regulação.

Figura 8: Síntese dos temas em cada polo dos discursos sobre regulação



Fonte: produção própria

Esta visualização opera como um diagrama de forças lexicais.

1. **O Eixo da disputa (centro):** a coluna central identifica os **conceitos neutros** (definição, Autoridade, Infraestrutura, Temporalidade) que estão sendo debatidos. A linha tracejada cinza representa a fronteira onde a regulação tenta se equilibrar.

2. **Perspectiva A (Azul - Esquerda):** Representa contribuintes que enfatizaram previsibilidade e flexibilidade operacional. Os termos recorrentes incluem 'medida formal', 'contextos de alto risco', 'neutralidade tecnológica'. Os argumentos associados enfatizam a necessidade de segurança jurídica.

3. **Perspectiva B (Vermelho - Direita):** Representa contribuintes que enfatizaram salvaguardas e controle público. Os termos recorrentes incluem 'garantia enfática', 'soberania de dados', 'emissor raiz'. Os argumentos associados enfatizam a necessidade de auditoria independente.

4. **O Vocabulário "*in vivo*":** Os termos em itálico são citações literais dos participantes. A visualização prova que palavras como "Harmonização" (Indústria) e "Soberania" (Sociedade Civil) são usadas para descrever o mesmo fenômeno (relação com normas externas), mas com vetores de força opostos.

4. ANÁLISE ESTRUTURAL E CONTEXTUAL

O quadro abaixo organiza as tensões identificadas na dinâmica de interesses no processo regulatório da verificação de idade.

Quadro Comparativo: Posições sobre Desenhos regulatórios (REGU)

DIMENSÃO DE ANÁLISE	SETOR PRIVADO	SOCIEDADE CIVIL E ACADEMIA	SÍNTESE DAS DIVERGÊNCIAS
Definição Normativa	**Clareza como previsibilidade:** Argumentos de que a taxatividade é necessária para restringir o escopo da lei a cenários de alto risco, criando zonas de não incidência. A subjetividade normativa é apontada como geradora de insegurança jurídica.	**Clareza como garantia:** Argumentos de que a definição estrita é necessária para impedir usos não autorizados de biometria e garantir a finalidade da coleta. A taxatividade é defendida como mecanismo de limitação da coleta de dados.	Ambos os setores defendem clareza normativa, mas com objetivos distintos: previsibilidade para conformidade versus limitação de práticas de coleta.
Fonte de Autoridade	**Padrões internacionais:** Argumentos favoráveis à adoção de tecnologias já aceitas por reguladores estrangeiros (Reino Unido, ICO), citando a experiência internacional como indicador de maturidade técnica.	**Adequação ao contexto nacional:** Argumentos de que a ANPD deve criar modelo adaptado à realidade brasileira, priorizando infraestrutura pública sobre soluções importadas.	Divergência sobre a referência preferencial: padrões internacionais consolidados versus modelo nacional autônomo.
Infraestrutura e Método	**Neutralidade tecnológica:** Argumentos favoráveis à flexibilidade e livre escolha de métodos, sustentando que a imposição de tecnologia específica cria barreiras à inovação e custos desproporcionais.	**Infraestrutura pública:** Argumentos favoráveis a APIs públicas, integração federada e arquitetura que garanta que dados não fiquem sob custódia exclusiva de empresas privadas.	Divergência sobre o papel do Estado: estabelecer requisitos mínimos sem prescrever soluções versus prover infraestrutura pública de verificação.
Governança e Auditoria	**Certificação técnica:** A auditoria é proposta como validação técnica por laboratórios independentes para atestar conformidade. Foco na acurácia dos algoritmos e testes de viés.	**Transparência e prestação de contas:** A auditoria é proposta como mecanismo de transparência pública, com publicação de relatórios que permitam escrutínio pela sociedade, não apenas pelo regulador.	Divergência sobre o objetivo da auditoria: certificação de conformidade técnica versus transparência pública e accountability.
Temporalidade e Implementação	**Implementação gradual:** Argumentos de que a aplicação imediata gera insegurança jurídica, solicitando diretrizes claras e prazos adequados como pré-requisitos para fiscalização.	**Prazos com compromisso:** Argumentos de que prazos de transição são necessários, mas não podem justificar inação ou adoção superficial. Defesa de que custos de conformidade não devem gerar assimetria entre	Divergência sobre a calibragem temporal: prazos mais longos para segurança jurídica versus prazos que não posterguem a proteção efetiva.

DIMENSÃO DE ANÁLISE	SETOR PRIVADO	SOCIEDADE CIVIL E ACADEMIA	SÍNTESE DAS DIVERGÊNCIAS
		grandes e pequenas plataformas.	

4. Comparação de Propostas de Modelos de Aferição

A maior parte dos participantes apenas discorreu sobre os métodos de aferição existentes, muitos tomando como base o Radar Tecnológico da ANPD, ou tecnologias que empresas específicas empregam. No entanto, poucos propuseram como estes métodos poderiam ser combinados ou utilizados na arquitetura da verificação de idade.

A análise a seguir apresenta as principais linhas específicas de verificação, a partir das propostas da Meta, do Instituto Alana, do Google, CGI.br e e-Sapiens, detalhando os aspectos técnicos e a cadeia de responsabilidades de cada modelo.

4.1 Consensos identificados

Embora os modelos regulatórios identificados partam de abordagens técnicas e conceituais diferentes, a análise transversal da categoria Desenho Regulatório revela a existência de um núcleo comum de viabilidade política, onde os interesses do setor privado e da sociedade civil convergem pragmaticamente, permitindo ao regulador avançar sem resistência estrutural.

No plano técnico, estabelece-se um consenso sobre a necessidade de interoperabilidade via interfaces de programação de aplicações (APIs), rejeitando-se a viabilidade de sistemas isolados. Para o mercado, essa padronização via APIs representa uma estratégia de eficiência econômica e redução de custos operacionais, permitindo o aproveitamento da infraestrutura já estabelecida pelos sistemas operacionais; simultaneamente, para a sociedade civil, a mesma arquitetura é defendida como mecanismo de democratização, viabilizando o acesso de pequenos desenvolvedores a validadores públicos, como o Gov.br, e garantindo a auditabilidade externa.

Metodologicamente, observa-se uma unanimidade na rejeição de regras uniformes (*one-size-fits-all*), consolidando a matriz de risco como o instrumento ordenador da verificação. Contribuintes do setor privado apoiam a escalabilidade das

exigências conforme o risco para evitar fricções desnecessárias em aplicações de baixo potencial ofensivo, preservando a usabilidade, enquanto a sociedade civil adere à mesma lógica sob a ótica da minimização de dados, argumentando que a coleta intensiva de informações é injustificável onde não há perigo real e imediato.

No aspecto temporal, o instituto do *sandbox* regulatório emerge como ponto de concordância absoluta, fundamentado na premissa de que a testagem deve preceder a sanção. O setor privado manifestou interesse em *sandboxes* para desenvolvimento e teste de soluções, ao passo que as organizações de defesa de direitos visualizam no *sandbox* a oportunidade de verificar empiricamente se as soluções propostas preservam, de fato, a privacidade dos usuários antes de sua massificação.

Por fim, no âmbito da governança, ambos os setores exigem segurança jurídica e diretrizes definitivas antes do início da fiscalização, diante da necessidade de clareza normativa. O mercado busca proteção contra passivos jurídicos decorrentes de interpretações divergentes, enquanto a sociedade civil visa evitar a fragmentação técnica que poderia enfraquecer a eficácia da proteção. Diante deste cenário de convergência, essas convergências indicam viabilidade para que a regulamentação estabeleça APIs como padrão técnico, estabelecer níveis graduais de risco, instituir regimes de *sandbox* imediatos e publicar guias técnicos orientadores, consolidando uma base normativa estável e politicamente sustentável.

4.2 Divergências identificadas

A análise das proposições revela a identificação de três modelos regulatórios distintos, cada um articulando uma filosofia de governança, um conjunto de expectativas técnicas e uma estrutura de responsabilidades.

O primeiro paradigma, denominado **regulação principiológica**, é sustentado pelo grupo de contribuintes do setor privado composto por Meta, Google, Microsoft, EA, Câmara-e.net e Brasscom. A filosofia central deste modelo postula que cabe ao Estado definir princípios orientadores gerais, enquanto o mercado deve reter a discricionariedade para definir os meios técnicos de implementação. A demanda fundamental é por uma estrutura normativa baseada em diretrizes flexíveis e não em regras prescritivas, garantindo às empresas autonomia na avaliação de risco. O efeito prático desta abordagem é a consolidação do controle técnico nas camadas de

infraestrutura, especificamente nos Sistemas Operacionais e Lojas de Aplicativos, atribuindo a essas empresas função de verificação centralizada dos sinais de idade e conferindo protagonismo à aprovação parental como mecanismo de conformidade. Este grupo manifestou oposição à rigidez normativa e à redundância de verificações. A contribuição da Meta propôs centralização no sistema operacional, modelo que reduziria obrigações no nível da aplicação. Em termos de implementação, exigem um período de *vacatio legis* estendido (12 meses) e o fomento a *sandboxes* regulatórios, opondo-se à imposição de soluções únicas ou à fiscalização punitiva durante períodos de instabilidade técnica. Nota-se uma nuance estratégica onde a contribuição da Meta propõe centralização no sistema operacional, o que teria como efeito prático a redução de obrigações no nível da aplicação, enquanto a Microsoft indicou disponibilidade para atuar como infraestrutura, condicionada à clareza sobre o regime de responsabilidade.

Em contraposição, o modelo de **auditoria e soberania**, defendido pela sociedade civil e órgãos de governança (Instituto Alana, CGI.br, FNPETI, Idec), estabelece os sistemas de verificação sejam submetidos a auditoria independente. O princípio orientador é a de que o Estado deve garantir a soberania digital e a auditabilidade externa dos sistemas. As demandas concentram-se na exigência de auditorias algorítmicas de vieses e na certificação rigorosa de fornecedores por terceiros independentes. Espera-se a construção de uma infraestrutura pública baseada em *blind APIs* e soluções gratuitas integradas a bases governamentais, rejeitando-se modelos de negócios baseados na monetização de dados ou que gerem interdependência indevida com entes privados. O modelo prescreve o controle social e a certificação como imperativos, vetando a confiança na autoavaliação corporativa e a retenção de dados biométricos. O efeito sistêmico desta proposta é o fortalecimento da privacidade e da governança pública, ainda que imponha custos elevados e prazos de implementação dilatados para a maturação da infraestrutura estatal (Gov.br).

Uma terceira via constitui o modelo de **harmonização técnica**, articulado pelos fornecedores de tecnologia de identidade (Yoti, Match Group, Unico). Este paradigma fundamenta-se na adoção de padrões globais e na certificação independente como mecanismos de legitimação. O objetivo é fomentar um mercado de terceiros de confiança (*ID Techs*) através da validação de tecnologias biométricas certificadas,

como o reconhecimento facial com prova de vida (*liveness*). As demandas giram em torno do alinhamento com estândares internacionais para evitar a fragmentação regulatória — regras peculiares locais — e a subjetividade nos critérios de fiscalização. Este grupo defende a eficácia medida por resultados e a estrita limitação de finalidade no uso de dados, opondo-se tanto ao banimento principiológico da biometria quanto à exigência de documentos oficiais para todas as interações.

A interseção destes modelos regulatórios com as opções de arquitetura revela três configurações de poder distintas. A combinação do **Modelo Principiológico** com a centralização na **Loja de Aplicativos** representa a arquitetura preferencial dos provedores de aplicação de internet: ao defender princípios flexíveis e a não redundância, legitima-se a verificação exclusiva no sistema operacional, transformando Apple e Google em "cartórios digitais" e eximindo os aplicativos de responsabilidade direta, embora essa arquitetura ignore a falha estrutural do compartilhamento de dispositivos, obscurecida pela autoavaliação de risco. Alternativamente, a fusão do **Modelo de Auditoria** com a **Responsabilidade em Cadeia** visa a Soberania Digital: a exigência de quebra da "caixa preta" das lojas e a demanda por *Blind APIs* forçam uma arquitetura federada onde a verificação ocorre via infraestrutura pública (Gov.br) e ZKP, enfrentando, contudo, o obstáculo da complexidade técnica de implementação. Por fim, a articulação do **Modelo de Harmonização Técnica** com a figura do **Terceiro Validador** resulta na terceirização do risco: ao estabelecer padrões de eficácia de alta precisão que as lojas de aplicativos não conseguem atender genericamente, obriga-se o aplicativo a contratar validadores externos especializados, estabelecendo um mercado de provedores de verificação, cuja tensão reside em preocupações manifestadas por organizações da sociedade civil quanto a soluções biométricas privadas não auditadas publicamente.

4.2.1. Modelo da garantia de idade centralizada

Este modelo foca na verificação a nível estrutural do ecossistema para evitar redundância de dados.

Funcionamento Técnico: Utiliza uma **API de Idade** que transmite sinais ou faixas etárias calculadas a partir da data de nascimento registada na conta do

dispositivo. Implementa a **Prevenção de Inferência de Aniversário**, mantendo o sinal antigo por um tempo aleatório após a data real para proteger a privacidade.

Cadeia de Responsabilidades:

- **Loja/SO:** Atua como o verificador raiz através de planos de telefonia 18+, cartões de crédito ou integração com o Gov.br. Fornece a API segura para os apps.
- **Pais:** Configuram a conta e estabelecem o vínculo, confirmando a idade do filho no dispositivo. Aprovam ou negam downloads via notificações remotas.
- **Desenvolvedor de App/App:** Integra a API e configura experiências padrão apropriadas a partir do sinal recebido. Deve monitorizar sinais conflituantes internos.

4.2.2 Modelo do método cachoeira (Cascata), Instituto Alana

Propõe uma sequência lógica baseada no risco, priorizando a minimização de dados.

Funcionamento Técnico: Aplica métodos do menos para o mais invasivo (inferência -> estimativa -> verificação determinística). O foco principal são as **Provas de Conhecimento Zero (ZKPs)** para provar a idade sem revelar a identidade civil.

Cadeia de Responsabilidades:

- **Loja/SO:** Deve oferecer suporte a perfis individuais ou máquinas virtuais alternativas no mesmo aparelho para isolar ambientes de crianças.
- **Pais:** Consentimento em **cinco etapas**: (1) identificação do responsável; (2) confirmação do vínculo; (3) captura do consentimento informado; (4) comunicação segura via token; (5) possibilidade de retirada do consentimento.

- **Desenvolvedor de App/App:** Realiza a aferição no nível do serviço. Em estimativas faciais, deve garantir o expurgo imediato e irreversível da imagem após o processamento.

4.2.3. Modelo de responsabilidade compartilhada e contextual

Rejeita uma solução única e foca na proteção “onde o usuário está”.

Funcionamento Técnico: Abordagem dinâmica em três categorias: (i) autodeclaração; (ii) estimativa; e (iii) verificação. Utiliza credenciais digitais e ZKPs para serviços que exigem maior certeza.

Cadeia de Responsabilidades:

- **Loja/SO:** Considerado apenas um dos atores; o Google alerta que esta camada falha em proteger crianças em navegadores web ou apps pré-instalados.
- **Pais:** Em dispositivos domésticos compartilhados (TVs, consolas), a supervisão parental é o pressuposto natural; verificação rigorosa contínua é inviável nestes casos.
- **Desenvolvedor de App/App:** Deve tomar medidas razoáveis para compreender a idade e aplicar proteções no nível de serviços individuais ou partes específicas do serviço.

4.2.4. Modelo de governança orientada por risco (4Cs)

Baseia-se na proporcionalidade e na interoperabilidade de padrões abertos.

Funcionamento Técnico: A verificação deve ser recorrente (“a cada acesso”) para conteúdos 18+ (pornografia, apostas). O SO envia um sinal de idade granular em faixas: **<12, 13-15, 16-17 ou 18+**.

Cadeia de Responsabilidades:

- **Loja/SO:** Fornecer sinais de idade via APIs seguras e interoperáveis. Implementar mecanismos para vincular contas de menores de 16 anos.

- **Pais:** Exercem supervisão parental ativa e voluntária. O modelo alerta para o risco de exclusão de famílias sem literacia digital ou acesso.

- **Desenvolvedor de App/App:** Deve avaliar o risco com base nos **4Cs**: Conteúdo, Contato, Conduta e Contrato. Devem garantir a possibilidade de desabilitar funcionalidades de IA não essenciais

4.2.5. Modelo do bloqueio parcial e treino de IA

Este modelo foi proposto por contribuinte do setor de verificação de idade, com foco em plataformas que hospedam conteúdo adulto, focando na viabilidade econômica e na precisão técnica através da inteligência artificial.

Funcionamento Técnico: Defende a **Autenticação em Conta** (vinculada ao cadastro/pagamento) em vez de verificações repetitivas a cada acesso. Inova ao propor o **bloqueio parcial (*blur*)**: o usuário não verificado pode acessar a plataforma, mas as funcionalidades de comunicação e o conteúdo visual explícito permanecem desfocados ou desabilitados até a comprovação da idade.

Cadeia de Responsabilidades:

- **Loja/SO:** Não é o foco central, mas a infraestrutura deve permitir o uso de dados para fins de segurança.

- **Pais:** Atuam indiretamente através do controle financeiro, já que muitas verificações neste modelo estão atreladas a meios de pagamento de assinaturas.

- **Desenvolvedor de App/App:** Deve implementar o mecanismo de "*blur*" (desfoque) na interface. A contribuição propôs o uso de dados biométricos para treinamento de IA, ressalvando vedação a uso comercial/publicitário. Tal posição foi contestada por contribuintes da sociedade civil, que apontaram riscos de desvio de finalidade.

PONTO DE ATUAÇÃO TÉCNICA	AÇÕES PRÁTICAS DOS PAIS	MECANISMO DE PROTEÇÃO DE DADOS	GATILHO DE ACIONAMENTO
Nível estrutural do Sistema Operacional (SO) e Lojas de Aplicativos	Vincular contas e aprovar ou negar downloads via notificações remotas.	Buffer aleatório de aniversário para impedir a dedução da data exata de nascimento.	Criação de conta no dispositivo e download de novos aplicativos.
Perfis de usuário isolados ou ambientes virtuais protegidos no dispositivo.	Consentimento em etapas: identificação, vínculo, informação, token e revogação.	Provas de Conhecimento Zero (ZKPs) e expurgo imediato de imagens biométricas.	Existência de riscos desproporcionais ou falha em método anterior de verificação.
Pontos de interação individual (navegadores, apps, *Smart TVs*).	Supervisão voluntária e gestão contextual em dispositivos compartilhados.	Credenciais anônimas e tecnologias de preservação de privacidade por design.	Acesso a serviços ou conteúdos destinados exclusivamente a adultos.
Nível da conta de usuário (assinatura) e interface da plataforma.	Controle de meios de pagamento (cartão de crédito) e acesso a contas pagas.	Algumas propostas incluíram permissão de uso de dados biométricos para aprimoramento de segurança, vedando perfilamento publicitário.	Acesso a conteúdo explícito desfocado ou uso de funcionalidades de comunicação direta.
Arquitetura interoperável via APIs abertas e padrões técnicos comuns.	Vinculação ativa de contas para menores de 16 anos e supervisão contínua.	Anonimização e vedação absoluta ao tratamento para fins comerciais.	Conteúdos legalmente restritos a maiores de 18 anos (apostas, conteúdo adulto) e interações via Inteligência Artificial.

4.3 Análise comparativa

O modelo de garantia de idade centrada no dispositivo e nas lojas de aplicativos funciona por meio de uma interface de programação chamada API de Idade que transmite apenas a faixa etária do usuário para os serviços digitais. A verificação ocorre uma única vez no nível estrutural do sistema operacional ou da loja de aplicativos durante a configuração inicial da conta do dispositivo.

Nesta cadeia de responsabilidades a loja de aplicativos e o sistema operacional atuam como o ponto de controle universal. Eles verificam a idade do titular da conta principal por meio de métodos como planos de telefonia operados por maiores de 18 anos ou processamento de pagamentos com cartão de crédito. A loja detém a data de nascimento completa e calcula a categoria etária (como menor de 12 anos) para compartilhar com os aplicativos sem revelar o dado bruto.

Os pais têm a tarefa de configurar a conta do menor e estabelecer o vínculo de supervisão. Eles fornecem a idade correta do filho e recebem notificações remotas em seus próprios aparelhos para aprovar ou negar o download de cada aplicativo solicitado pelo adolescente. Esta estrutura permite que os responsáveis gerenciem o acesso de forma centralizada sem repetir o processo em cada serviço.

O desenvolvedor de aplicativos precisa integrar a API de Idade em seu código para solicitar as faixas etárias permitidas. O aplicativo que recebe o sinal deve então configurar automaticamente as experiências apropriadas para aquela idade. Ele mantém o dever de monitorar comportamentos que conflitem com o sinal recebido e de aplicar salvaguardas internas de segurança.

O Instituto Alana defende o Método Cachoeira ou Técnica de Cascata para a aferição etária. O funcionamento segue uma aplicação sequencial de múltiplos mecanismos que inicia com métodos de baixa fricção e menor invasividade. O sistema prioriza a inferência ou estimativa e escala para métodos determinísticos apenas quando os resultados iniciais são inconclusivos.

A cadeia de responsabilidades do Alana exige uma análise de risco proporcional para cada serviço. Os pais participam de um processo de consentimento parental em cinco etapas rigorosas. A primeira etapa é a identificação do responsável legal. A segunda consiste na confirmação do vínculo entre o adulto e a criança. A terceira etapa requer a captura do consentimento informado sobre o uso dos dados. A quarta envolve a comunicação segura do status de autorização por meio de um token ou sinal criptográfico. A quinta etapa garante a possibilidade de retirada do consentimento a qualquer momento pelo responsável.

A loja de aplicativos e o sistema operacional devem oferecer suporte nativo para múltiplos perfis no mesmo aparelho. Eles precisam permitir a criação de ambientes isolados onde as restrições são ativadas apenas no contexto do perfil da criança. O aplicativo tem a obrigação técnica de utilizar provas de conhecimento zero para confirmar a idade sem coletar ou armazenar dados pessoais sensíveis.

No modelo baseado numa abordagem contextual e distribuída, a proteção deve ocorrer onde o usuário está no momento do acesso seja em navegadores ou aplicativos. O sistema utiliza três categorias gerais: autodeclaração para riscos baixos estimativa de idade para níveis médios e verificação de documentos apenas para serviços de alto risco.

Nesta cadeia a loja de aplicativos e o sistema operacional são vistos apenas como uma das camadas de proteção. O Google argumenta que focar apenas neles falha em proteger crianças que acessam a rede via navegadores web ou aplicativos pré-instalados em dispositivos compartilhados. Os pais exercem uma supervisão natural baseada no uso doméstico em aparelhos como *Smart TVs* e consoles de videogame.

O desenvolvedor de app deve aplicar medidas razoáveis para compreender a idade do público no contexto específico do seu produto. O app assume a responsabilidade direta de restringir o acesso a conteúdos impróprios de forma proporcional à sua funcionalidade. A verificação rigorosa fica limitada a serviços destinados exclusivamente a adultos para evitar a coleta desnecessária de dados de menores.

No modelo da governança multissetorial e da responsabilidade compartilhada entre todos os agentes digitais, o funcionamento técnico segue uma matriz que avalia Conteúdo, Contato, Conduta e Contrato. Para serviços de alto risco como pornografia e apostas o sistema exige verificação rigorosa a cada acesso proibindo apenas a autodeclaração. Nos outros casos a aferição ocorre pelo compartilhamento de sinais de idade por meio de interfaces técnicas abertas e interoperáveis.

Nesta estrutura os provedores de sistemas operacionais e lojas de aplicativos devem fornecer meios seguros para transmitir sinais de idade a terceiros. Eles precisam garantir a privacidade por padrão em todos os processos de execução. Cabe a esses agentes oferecer ferramentas que ajudem os pais a vincular as contas de menores de dezesseis anos para supervisão. Os pais assumem o dever de participar ativamente da orientação dos menores no ambiente digital. Eles usam as ferramentas de vinculação de contas e supervisão parental das plataformas para gerir o acesso e a segurança dos filhos. O desenvolvedor de aplicação deve realizar sua avaliação de

riscos específica para o serviço oferecido. O aplicativo não pode se omitir baseando-se apenas no sinal da loja se o serviço apresentar riscos de contato ou conduta inadequada. Ele precisa aplicar salvaguardas técnicas proporcionais aos danos potenciais identificados na matriz.

As convergências entre os modelos residem no reconhecimento do melhor interesse da criança e na necessidade de proporcionalidade técnica baseada no risco. Quase todas as propostas defendem a minimização da coleta de dados e o uso de sinais criptográficos ou APIs para preservar o anonimato. As divergências surgem na centralidade da verificação. Enquanto há quem priorize o sistema operacional como o único ponto de verdade para reduzir o cansaço do usuário, outros advertem que soluções focadas apenas em lojas ignoram o acesso por navegadores *web* e aparelhos compartilhados. O Alana distingue-se pela exigência de uma prova de idade em cascata e pelo uso estrito de provas de conhecimento zero para impedir a vigilância estatal ou comercial. Enquanto há quem defenda, de um lado, um fluxo de retorno de informações de idade para o sistema operacional, do outro, há quem enfatize auditorias independentes e controle social para evitar abusos na infraestrutura de aferição.

ANEXO A - SUMÁRIO DO CODEBOOK DA ANÁLISE QUALITATIVA

CATEGORIA: ADEQUAÇÃO E PROPORCIONALIDADE (ADEQ)

Argumentos sobre princípios de calibração da regulação.

CÓDIGO	DEFINIÇÃO OPERACIONAL
ADEQ_ALTO_RISCO_RIGO	Argumentos de que serviços de alto risco devem estar sujeitos a verificação robusta ou documental.
ADEQ_BAIXO_RISCO_FLEX	Argumentos de que serviços de baixo risco devem estar sujeitos a métodos de verificação simplificados.
ADEQ_EDUCACAO	Argumentos de que soluções técnicas são insuficientes sem políticas complementares de educação midiática e digital.
ADEQ_MINIMIZACAO	Argumentos favoráveis à coleta mínima de dados, limitada ao estritamente necessário para a verificação de idade.
ADEQ_OFFLINE_INCL	Argumentos favoráveis a mecanismos de validação presencial ou assistida para evitar exclusão digital.
ADEQ_PRIV_ZKP	Argumentos de que arquiteturas baseadas em Prova de Conhecimento Zero são a solução preferencial para conciliar verificação e privacidade.

CATEGORIA: ARQUITETURA DE IMPLEMENTAÇÃO (ARQ)

Argumentos sobre o ponto da cadeia de valor em que a verificação deve ocorrer.

CÓDIGO	DEFINIÇÃO OPERACIONAL
ARQ_APP_LEVEL	Argumentos de que a verificação deve ocorrer no nível da aplicação ou site, permitindo controle contextual pelo desenvolvedor.
ARQ_CADA_ACESSO	Discussões sobre a exigência de verificação a cada acesso, especialmente para serviços de alto risco.
ARQ_CADASTRO_UNICO	Argumentos favoráveis à verificação única no momento do cadastro, sem necessidade de revalidação posterior.
ARQ_CADEIA_RESP	Discussões sobre a distribuição de responsabilidades na cadeia de valor digital (desenvolvedores, plataformas, lojas de aplicativos).
ARQ_DISPOSITIVO_PART	Discussões sobre o desafio dos dispositivos compartilhados por múltiplos usuários, que dificultam a verificação baseada em conta única.
ARQ_LOJA_APPS	Argumentos de que a verificação deve ocorrer no nível da Loja de Aplicativos ou Sistema Operacional.

CATEGORIA: DESENHO REGULATÓRIO (REGU)

Argumentos sobre a estrutura jurídica, temporal e institucional da norma.

CÓDIGO	DEFINIÇÃO OPERACIONAL
REGU_API_ABERTA	Argumentos favoráveis a APIs abertas e interoperabilidade entre sistemas de verificação.
REGU_CERTIF_AUDITAB	Propostas de acreditação, auditoria ou certificação oficial de fornecedores de tecnologia de verificação.
REGU_COMPLEXIDADE	Preocupações com burocracia, complexidade normativa ou insegurança jurídica.
REGU_HARMONIZACAO	Argumentos sobre a necessidade de alinhamento com legislação nacional (LGPD) e marcos internacionais.
REGU_NEUTRALIDADE	Argumentos de que a regulamentação não deve prescrever tecnologias específicas, mantendo neutralidade tecnológica.
REGU_ORIENT_DEF	Solicitações de definições claras, orientações ou princípios específicos por parte do regulador.
REGU_PRAZOS	Solicitações de extensão de prazos, período de carência ou implementação gradual das obrigações.
REGU_SANDBOX	Propostas de ambientes de teste experimentais (sandbox regulatório) ou projetos-piloto.

CATEGORIA: DIAGNÓSTICO E RESPONSABILIDADE (DIAG)

Argumentos sobre a origem do problema e a legitimidade da intervenção regulatória.

CÓDIGO	DEFINIÇÃO OPERACIONAL
DIAG_CETICISMO_DANOS	Questionamentos sobre a necessidade ou eficácia da regulação proposta, incluindo argumentos sobre insuficiência de evidências empíricas.
DIAG_DEVIDA_DILIGENCIA	Argumentos de que a obrigação das empresas deve ser de meios (melhores esforços) e não de resultado.
DIAG_FALHA_AUTO	Argumentos de que o modelo atual de autodeclaração é insuficiente ou ineficaz para contextos de alto risco.
DIAG_PRIMAZIA_FAMILIAR	Argumentos que enfatizam o papel da supervisão parental como elemento central da proteção, com a tecnologia de verificação atuando como complemento.
DIAG_RESP_SOLIDARIA	Argumentos de que a proteção é dever compartilhado entre Estado, empresas e família, conforme art. 227 da Constituição Federal.

CATEGORIA: ESCOPO E MODULAÇÃO SETORIAL (ESCO)

Argumentos sobre quais serviços devem ser objeto de regulação e em que intensidade.

CÓDIGO	DEFINIÇÃO OPERACIONAL
ESCO_CONTEUDO_PROIBIDO	Argumentos de que a verificação robusta deve aplicar-se apenas a conteúdos legalmente restritos a maiores de 18 anos (ex: pornografia, apostas).
ESCO_DEF_RISCO	Discussões sobre critérios para classificação de risco, incluindo design de engajamento, possibilidade de interação com desconhecidos e tipologia dos 4Cs.
ESCO_GATEKEEPERS	Argumentos de que as obrigações devem ser proporcionais ao porte e capacidade das empresas, com exigências mais rigorosas para grandes plataformas.
ESCO_ISENCAO_EDITORIAL	Argumentos para tratamento diferenciado de serviços com curadoria editorial (jornalismo, plataformas de vídeo sob demanda).
ESCO_ISENCAO_FINANCEIRO	Argumentos para tratamento diferenciado do setor financeiro, que já opera sob regime de verificação de identidade (KYC).
ESCO_ISENCAO_PROFISSIONAL	Argumentos para tratamento diferenciado de plataformas de networking profissional e emprego.
ESCO_MATRIZ_RISCO	Argumentos favoráveis ao escalonamento das exigências conforme o nível de risco do serviço.

ARGUMENTOS DE LEGITIMAÇÃO (LEGIT)

Argumentos utilizados pelos contribuintes para fundamentar suas posições.

CÓDIGO	DEFINIÇÃO OPERACIONAL REVISADA
LEGIT_CONFORMIDADE	Argumentos de que as empresas já cumprem a legislação vigente (LGPD, ECA) e que novas regras seriam redundantes.
LEGIT_INCLUSAO	Argumentos de que determinadas tecnologias (ex: estimativa facial) promovem inclusão social por não exigirem documentos oficiais.
LEGIT_EXPERIENCIA	Argumentos de que a usabilidade e a fluidez da navegação devem ser consideradas na regulamentação.
LEGIT_INFRAESTRUTURA	Argumentos favoráveis ao desenvolvimento de soluções brasileiras de verificação, reduzindo dependência de infraestrutura estrangeira.
LEGIT_VALOR_SOCIAL	Argumentos de que determinadas plataformas oferecem conteúdo educativo ou benefícios sociais que justificariam tratamento diferenciado.

CATEGORIA: IMPACTOS E BARREIRAS (IMPACT)

Preocupações com consequências práticas e econômicas da implementação.

CÓDIGO	DEFINIÇÃO OPERACIONAL REVISADA
IMPACT_AUTONOMIA_JUVENIL	Preocupações com impacto sobre a autonomia progressiva e a privacidade de adolescentes (16-17 anos).
IMPACT_BARREIRA_PME	Preocupações com custos de conformidade que podem representar barreira significativa para pequenas e médias empresas.
IMPACT_CUSTO_CONS	Preocupações com possível repasse dos custos de verificação ao consumidor final.
IMPACT_EXCLUSAO_DIG	Preocupações com exclusão digital de populações vulneráveis ou sem documentação formal.
IMPACT_FISCALIZ	Discussões sobre desafios práticos de fiscalização e barreiras institucionais para aplicação da norma.
IMPACT_FRICCAO_USUARIO	Preocupações com impacto na experiência do usuário, incluindo possível abandono do serviço.
IMPACT_LITERACIA_FAMILIAR	Preocupações com eficácia limitada em razão da falta de competência técnica dos pais ou responsáveis.
IMPACT_MERCADO_PARALELO	Preocupações com migração de usuários para plataformas não reguladas ou de origem não identificada.

CATEGORIA: RISCOS ESPECÍFICOS (RISC)

Preocupações com ameaças à privacidade e segurança decorrentes da implementação.

CÓDIGO	DEFINIÇÃO OPERACIONAL REVISADA
RISC_EFICACIA_EVASAO	Questionamentos sobre a eficácia da verificação diante de possibilidades técnicas de evasão (VPNs, documentos falsos).
RISC_HONEYPOT	Preocupações com a criação de bases de dados centralizadas que se tornam alvos prioritários para ataques cibernéticos.
RISC_MINERACAO_COMERCIAL	Preocupações com desvio de finalidade, onde dados de verificação sejam utilizados para perfilamento comercial.
RISC_REID_CRUZADA	Preocupações com reidentificação de usuários através do cruzamento de metadados.
RISC_TREINO_IA	Preocupações com uso não autorizado de dados para treinamento de modelos de Inteligência Artificial.

CÓDIGO	DEFINIÇÃO OPERACIONAL REVISADA
RISC_VIGILANCIA_ESTADO	Preocupações de que a infraestrutura de verificação possa ser utilizada para vigilância ou controle estatal.

CATEGORIA: SOLUÇÕES TÉCNICAS E MÉTODOS (TECH)

Discussões sobre ferramentas tecnológicas específicas de verificação de idade.

CÓDIGO	DEFINIÇÃO OPERACIONAL REVISADA
TECH_AUTODEC_VALIDA	Discussões sobre autodeclaração de idade, incluindo argumentos favoráveis e contrários, frequentemente proposta como camada inicial em modelos escalonados.
TECH_CONTROLE_PARENTAL	Discussões sobre ferramentas de controle parental como mecanismo complementar ou alternativo à verificação direta.
TECH_DADO_BANCARIO	Discussões sobre uso de informações bancárias ou de cartão de crédito (Open Banking) para verificar maioridade civil.
TECH_DOC_OFICIAL	Discussões sobre verificação documental tradicional (envio de RG, CNH ou Passaporte).
TECH_ESTIMATIVA_FACIAL	Discussões sobre estimativa de idade por análise de imagem facial, sem identificação civil.
TECH_GOV_INFRA	Discussões sobre uso de bases de dados governamentais (Gov.br, SERPRO) como fonte de validação.
TECH_INFERENCIA_IA	Discussões sobre inferência algorítmica de idade por análise comportamental ou histórico de navegação.
TECH_TERCEIRO_VALIDADOR	Discussões sobre recurso a empresas especializadas em verificação de identidade como intermediários.
TECH_ZKP_TOKEN	Discussões sobre tecnologias de preservação de privacidade (Prova de Conhecimento Zero), tokens anonimizados e credenciais verificáveis.

ANEXO B. LISTA DE CONTIBUINTES DA CONSULTA PÚBLICA

Além de 20 contribuições feitas em nome de pessoas físicas (cidadãos, especialistas e acadêmicos), segue a relação das pessoas jurídicas que encaminharam respostas à Consulta Pública:

Apple Computer Brasil

Associação Alquimídia, a primeira organização em defesa do Fediverso no Brasil

Associação Brasileira da Indústria Elétrica e Eletrônica (ABINEE)

Associação Brasileira das Empresas de Software (ABES)

Associação Brasileira de Anunciantes (ABA)

Associação Brasileira de Defesa do Consumidor (PROTESTE)

Associação Brasileira de Emissoras De Rádio E Televisão (ABERT)

Associação Brasileira de Mobilidade e Tecnologia (AMOBITEC)

Associação das Empresas de Tecnologia da Informação e Comunicação e de Tecnologias Digitais (BRASSCOM)

Associação de Software de Entretenimento (ESA)

Aylo

Câmara Brasileira da Economia Digital (Camara-e.net)

Centro de Tecnologia e Sociedade (CTS-FGV Direito Rio)

Claro S.A.

Coalizão Direitos na Rede

Comitê Gestor da Internet (CGI.br)

Confederação Nacional das Seguradoras (CNseg)

DiraCom – Direito à Comunicação e Democracia

Electronic Arts

Electronic Frontier Foundation (EFF)

Epic Games

eSapiens Tecnologia S.A.

Family Talks - Associação de Desenvolvimento da Família

Febraban e Abecs (Associação Brasileira das Empresas de Cartões de Crédito e Serviços)

Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo

Fórum Nacional de Prevenção e Erradicação do Trabalho Infantil e Proteção a Adolescentes no Trabalho (FNPETI)

Google Brasil Internet LTDA

IBRAC - Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional

Idwall Tecnologia

Instituto Alana

Instituto de Defesa de Consumidores (Idec)

Instituto de Tecnologia e Sociedade do Rio

Instituto Teckids

Internet Society - Capítulo Brasil

Kaspersky Lab Soluções Seguras Brasil LTDA

LinkedIn

MatchGroup (Tinder)

Microsoft

Ministério Público Federal - Comissão de Tecnologia da Informação e Comunicação da 3a. Câmara de Coordenação e Revisão

Motion Picture Association - Brasil

Roblox

Roku

Samsung Eletrônica da Amazônia LTDA.

SHPS Tecnologia e Serviços

STRIMA

Tools for Humanity

Unico - IDTech

Wikimedia Foundation & Wikimedia Brasil

Yoti

Zetta

MINISTÉRIO DA
JUSTIÇA E
SEGURANÇA PÚBLICA

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO