Contribuições do Debatedor Ergon Cugler, Conselheiro da Presidência da República no Conselho de Desenvolvimento Econômico Social Sustentável (CDESS) para o Grupo de Trabalho sobre Proteção de Crianças e Adolescentes em Ambiente Digital

24 de setembro de 2025

Ergon Cugler de Moraes Silva, 27 anos, pesquisador CNPq sobre desinformação, inteligência artificial e tecnologias. Conselheiro da Presidência da República no Conselho de Desenvolvimento Econômico Social Sustentável (CDESS), o "Conselhão" do Governo Federal (2025-2027). Graduado em Gestão de Políticas Públicas pela Universidade de São Paulo (USP) e Pós-Graduado em Data Science & Analytics também pela USP. Possui Mestrado em Administração Pública e Governo pela Fundação Getulio Vargas (FGV) e Pós-Graduação em Data Science for Social & Business Analytics pela Universitat de Barcelona (UB). Atua na ONG More in Common e no Laboratório de Estudos sobre Desordem Informacional e Políticas Públicas (DesinfoPop/FGV).

Ideia central: Devemos garantir segurança sem ameaçar a privacidade; Devemos garantir verificação etária, sem ameaçar verificação de identidade.

1) Contexto: o modelo autodeclaratório das companhias falhou

Plataformas que dependem do próprio usuário "dizer a idade" (e depois tentar rastrear os menores com sinais indiretos). Esse modelo tem apresentado diversas limitações, vide:

- No levantamento oficial da eSafety australiana com oito serviços digitais, constatou-se que 80% das crianças de 8 a 12 anos utilizaram redes sociais em 2024, mesmo com a idade mínima geralmente fixada em 13 anos. Apenas 10% das que tinham conta relataram ter tido o perfil derrubado por idade entre janeiro e setembro de 2024, revelando a baixa efetividade dos mecanismos de controle atualmente aplicados[1]. O relatório mostra ainda

[1] AUSTRALIA. eSafety Commissioner. Behind the screen: The reality of age assurance and social media access for young Australians – Transparency report. 2025. Disponível em: https://www.esafety.gov.au/research/children-and-social-media. Acesso em: 23 set. 2025.

que muitas plataformas seguem iniciando o processo de verificação apenas pela autodeclaração da idade e, em seguida, recorrem a métodos heterogêneos e pouco consistentes para tentar inferir a idade real dos usuários, como classificadores automáticos, análise de linguagem ou estimativas faciais[2]. No Brasil, a pesquisa TIC Kids Online do NIC.br/Cetic.br indica um cenário equivalente: 83% das crianças e adolescentes de 9 a 17 anos possuem perfil em pelo menos uma rede social, sendo que, entre 9 e 10 anos, 60% já estão nesses ambientes virtuais[3].

- No Reino Unido, a entrada em vigor do Online Safety Act trouxe obrigações claras para que serviços online, incluindo sites adultos, adotassem medidas robustas de verificação etária a fim de impedir o acesso de menores[4]. Na prática, a intensificação da aplicação regulatória resultou em dois efeitos visíveis: de um lado, houve aumento no uso de ferramentas de contorno, como VPNs, por parte de adolescentes para driblar bloqueios; de outro, abriu-se um debate intenso sobre proporcionalidade, privacidade e eficácia dos mecanismos. Isso mostrou que barreiras rígidas, centralizadas ou pouco diversificadas não eliminam o problema e ainda podem produzir efeitos colaterais, como exclusão indevida de maiores de idade ou estímulo à busca de serviços menos seguros[5].

- De acordo com a Ofcom, no material de orientação publicado para implementação do Online Safety Act, a simples autodeclaração da idade não é reconhecida como forma válida de verificação ou de estimação etária, já que não garante qualquer nível de certeza quanto à idade real do usuário e, portanto, não atende ao objetivo regulatório de impedir o acesso de crianças a conteúdos nocivos[6]. Essa diretriz é coerente com a síntese comparada que elaboramos a partir da legislação internacional, onde está registrado que medidas que "exigem que o usuário auto-declare sua própria idade" não são enquadradas como verificação nem como estimação, sendo explicitamente excluídas como mecanismos aceitáveis no contexto do OSA/UK. Essa posição é relevante porque obriga serviços digitais a irem além do mero campo de preenchimento de data de nascimento, adotando técnicas mais robustas de garantia etária, como verificação documental, estimação por modelos técnicos ou integração com identidades digitais confiáveis.

---

[2] 5RIGHTS FOUNDATION. But how do they know it is a child? Age Assurance in the Digital World. 2021. Disponível em: https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf. Acesso em: 23 set. 2025.

[3] BRASIL. NIC.br; Cetic.br. TIC Kids Online Brasil 2024. 2024. Disponível em: https://cetic.br/pt/pesquisa/kids-online. Acesso em: 23 set. 2025.

[4] REINO UNIDO. Online Safety Act 2023. UK Parliament, 2023. Disponível em: https://bills.parliament.uk/bills/3137. Acesso em: 23 set. 2025.

[5] EUROPEAN COMMISSION. Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of the Digital Services Act. 2025. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0607. Acesso em: 23 set. 2025.

[6] OFcom. Online Safety Act: quick guide to age assurance. 2023. Disponível em: https://www.ofcom.org.uk/online-safety. Acesso em: 23 set. 2025.

Conclusão prática: deixar a verificação privada e autodeclaratória nas mãos de cada serviço produz inconsistência, incentiva fraude e não atende ao padrão de "altamente efetivo" exigidos.

2) Arquitetura e conceitos: Onde, como, quando e o quê

2.1 Onde verificar (camadas possíveis)

1. **Camadas mais centralizadas**

   a) Chip/dispositivo (SIM/eSIM), dispositivo em si e sistema operacional. Vantagens: cobertura ampla. Fragilidades: no Brasil é comum o compartilhamento familiar de aparelhos e a posse desigual de telefone entre crianças e adolescentes leva ao risco de "colagem" da identidade do dono do chip ao uso de todos no aparelho. Em outras palavras: Uma criança poderá usar o celular da mãe e acessar conteúdos inadequados. Dados do Brasil mostram que a posse de celular próprio cresce com a idade, mas permanece incompleta entre os mais novos, o que cria vieses de exclusão se o chip vira pré-requisito universal", como aponta a pesquisa TIC Kids Online Brasil, realizada pelo Cetic.br/NIC.br. A edição de 2023 mostra que, entre crianças de 9 a 10 anos, apenas 47% tinham celular próprio, contra 91% na faixa de 15 a 17 anos, revelando desigualdade no acesso individualizado a dispositivos móveis.

   b) Loja de aplicativos. Vantagem: um só ponto de integração por ecossistema. Fragilidades: concentração de poder e travas concorrenciais, atualização cara e massiva para sites e serviços web que não passam por app stores. E, além disso, cobriria apenas aplicativos e os navegadores ficariam de fora.

2. **Camadas descentralizadas**

   a) No próprio aplicativo/serviço. No nível do próprio aplicativo ou serviço, a verificação etária acontece diretamente no ponto de maior risco: o site ou app que disponibiliza o conteúdo ou produto restrito. Vantagem: Essa abordagem tem a grande vantagem de ser proporcional ao risco, porque só é exigida de quem realmente oferece serviços sensíveis, como pornografia, apostas, venda de álcool ou jogos de azar. Isso evita impor barreiras universais a todos os usuários da internet e concentra os custos e responsabilidades em quem gera maior potencial de dano. Além disso, por estar no próprio serviço, há maior flexibilidade regulatória: a autoridade pode definir requisitos mínimos e auditar se cada plataforma está cumprindo, sem depender de terceiros globais como sistemas operacionais ou lojas de aplicativos. Fragilidades: A crítica é que esse modelo pode fragmentar a experiência do usuário, já que cada serviço teria seu próprio processo de checagem, obrigando o indivíduo a repetir várias vezes a prova de idade. Também há o risco de multiplicação da coleta de dados pessoais, pois cada site ou app poderia pedir documentos ou biometria. Porém, isso pode ser mitigado se a regulação incentivar padrões técnicos comuns, como uso de tokens de idade reutilizáveis ou soluções auditadas que devolvam apenas o atributo necessário ("maior de 18"), sem expor dados sensíveis.

2.2 Garantia, verificação e estimação: três coisas diferentes

- **Garantia etária (age assurance)** é o "guarda-chuva": conjunto de estratégias para saber se a experiência é apropriada e se o usuário está numa faixa etária.
- **Verificação etária** é quando se atesta idade exata ou um limiar (ex.: 18+).
- **Estimação etária** é inferir idade ou faixa provável sem documento, por sinais (ex.: biometria facial, linguagem, comportamento). **Exige cautela por precisão, vieses e proporção.**

2.3 Princípios regulatórios de referência

- Diretrizes do art. 28 do DSA (UE) pedem alto nível de privacidade e segurança para menores **por design e por padrão**, com medidas "state of the art", proporcionais, não intrusivas e com mínima coleta. Também exigem governança e revisão contínua.
- ARCOM França exige independência do verificador, confidencialidade e a chamada "dupla confidencialidade" (**o site não sabe quem você é nem o verificador sabe a que site você foi**). É a base técnica para certificados efêmeros e contra rastreio entre sites.

2.4 Certificados efêmeros x certificados únicos

- **Certificado único e reusável:** o usuário prova sua idade uma vez e pode reutilizar a credencial em diferentes plataformas. Vantagem: válido para múltiplos serviços, tem como atrativo a praticidade. Fragilidades: Porém, esse modelo gera um risco elevado de correlação entre serviços, já que o mesmo identificador pode ser rastreado em vários contextos, criando um perfil "pan-rede" que expõe hábitos de navegação e consumo. Isso abre espaço para abusos comerciais ou vigilância indevida.
- **Certificados efêmeros (um token por sessão ou por site)** funcionam como chaves descartáveis, a cada sessão ou a cada site, o usuário gera um token novo que apenas confirma o atributo necessário, por exemplo, "maior de 18 anos". Vantagem: esse desenho reduz drasticamente a possibilidade de rastreamento e de vinculação entre diferentes serviços, já que não há um identificador fixo. França[7] e União Europeia[8] avançam nesse caminho, apostando em mecanismos de "dupla confidencialidade" (onde nem o provedor de conteúdo sabe quem é o usuário, nem o verificador de idade sabe quais sites ele acessa) e em provas seletivas que compartilham somente a informação estritamente necessária. Esse movimento dialoga com a construção de uma solução interoperável no âmbito do

---

[7] FRANÇA. Autorité de Régulation de la Communication Audiovisuelle et Numérique (ARCOM). Référentiel technique sur la vérification de l'âge. Paris, 2024. Disponível em: https://www.arcom.fr/nos-ressources/etudes-et-donnees/mediatheque/frequentation-des-sites-adultes-par-les-mineurs. Acesso em: 23 set. 2025.

[8] UNIÃO EUROPEIA. Comissão Europeia. Guidelines pursuant to Article 28 of the Digital Services Act. Bruxelas, 2025. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification. Acesso em: 23 set. 2025.

eIDAS 2.0[9], em que a carteira de identidade digital europeia poderá servir também como prova seletiva de atributos, inclusive a idade, sempre com controle granular pelo usuário sobre o que é revelado. Fragilidades: Como cada certificado efêmero é descartável, o usuário pode ser obrigado a refazer a prova de idade em diferentes serviços, gerando fricção e perda de conveniência. Contudo, esse efeito pode ser reduzido se houver padrões técnicos comuns que permitam tokens efêmeros interoperáveis, armazenados temporariamente em carteiras digitais ou navegadores, de modo que a cada site seja transmitida apenas a informação mínima necessária ("maior de 18"), sem expor dados pessoais e sem repetir todo o processo.

3) O que NÃO queremos

A seguir, um mapa por método, explicando por que evitá-lo como solução principal. Em cada item trago o porquê, fragilidades e um exemplo internacional.

1. **Autodeclaração de idade**
    - **Porquê não:** não é verificação; é facilmente burlada; comprovadamente ineficaz na prática. a Austrália, 80% das crianças de 8 a 12 anos utilizaram redes sociais em 2024, mesmo com a idade mínima geralmente fixada em 13 anos. Apenas 10% das que tinham conta relataram ter tido o perfil derrubado por idade entre janeiro e setembro de 2024, revelando a baixa efetividade dos mecanismos de controle atualmente aplicados[10]. No Brasil, 83% das crianças e adolescentes de 9 a 17 anos possuem perfil em pelo menos uma rede social, sendo que, entre 9 e 10 anos, 60% já estão nesses ambientes virtuais[11], mesmo a maioria das plataformas dizendo que aceitam apenas a partir de 13 anos de idade.
2. **Cartão de crédito como "prova de adulto"**
    - **Porquê não:** não é inclusivo (muitos adultos não têm cartão; menores podem usar cartão dos pais); abre risco de *phishing* e de coleta de dados financeiros desnecessária; transfere o problema para setor bancário. Além disso, pesquisa apontou que 60% dos brasileiros de baixa renda não possuem cartão de crédito[12].

---

[9] UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Regulation (EU) on European Digital Identity (eIDAS 2.0). Bruxelas, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183. Acesso em: 23 set. 2025.

[10] AUSTRALIA. eSafety Commissioner. Behind the screen: The reality of age assurance and social media access for young Australians – Transparency report. 2025. Disponível em: https://www.esafety.gov.au/research/children-and-social-media. Acesso em: 23 set. 2025.

[11] BRASIL. NIC.br; Cetic.br. TIC Kids Online Brasil 2024. 2024. Disponível em: https://cetic.br/pt/pesquisa/kids-online. Acesso em: 23 set. 2025.

[12] FAST COMPANY BRASIL. Baixa renda ainda está distante do cartão de crédito e até do Pix. 2023. Disponível em: https://fastcompanybrasil.com/money/baixa-renda-ainda-esta-distante-do-cartao-de-credito-e-ate-do-pix/. Acesso em: 23 set. 2025.

3. **Upload de documento de identidade direto para cada site**

    - **Porquê não:** risco de vazamento, incentivo a bases privadas de dados biográficos, exclusão de jovens sem documentação; gera custo e atrito para todos. A síntese aponta esses riscos e que "provar ser adulto" faz mais sentido em serviços 18+, mas não para outras faixas etárias. Também pode ser relativamente fácil de fraudar, ao portar um documento de terceiros.

4. **Biométricos de IDENTIDADE (reconhecimento facial para identificar a pessoa ou CPF)**

    - **Porquê não:** coleta altamente sensível, risco de uso secundário, exclusão e vieses; não é necessário "saber quem" para "saber se é 18+". Diretrizes europeias priorizam minimização e seletividade. Risco de discriminação, ou pessoas com deficiência prejudicadas. Exemplo internacional: debates na Austrália destacaram riscos de viés e precisão em propostas de verificação facial. Também pode ser fácil de fraudar, ao utilizar imagens com inteligência artificial para burlar a identificação, tal como golpistas clonam cartões.

5. **Estimação facial de IDADE (sem identificação) como solução principal**

    - **Porquê não:** melhora a privacidade em relação ao reconhecimento facial, mas ainda traz desafios de precisão (sobretudo nas idades de limiar 12/13 e 17/18), viés e necessidade de *liveness*. Além da margem de erro ser realmente arriscada, há também risco de discriminação, ou pessoas com deficiência prejudicadas. Também pode ser fácil de fraudar, ao utilizar imagens com inteligência artificial para burlar a identificação, tal como golpistas clonam cartões.

6. **Verificação COMPORTAMENTAL (padrões de uso, escrita, rede social, horário etc.)**

    - **Porquê não:** intrusiva por definição, depende de perfis extensivos, sujeita a erro e discriminação. Deve ser evitada como meio principal.

7. **Testes de CAPACIDADE (quizzes de conhecimento, "maturidade" ou lógica)**

    - **Porquê não:** medem escolaridade, letramento ou familiaridade cultural, não idade; podem excluir crianças com deficiências e, ao mesmo tempo, ser vencidos por crianças "treinadas".

8. **SIM/Chip da linha telefônica**

    - **Porquê não:** telefone é frequentemente compartilhado no domicílio; nem todos menores possuem SIM próprio; atrela identidade da conta da linha a todo uso no dispositivo. No Brasil, a posse de celular próprio cresce com a idade e não é universal, o que cria exclusão se o chip vira o "gate". No Brasil é comum o compartilhamento familiar de aparelhos e a posse desigual de telefone entre crianças e adolescentes leva ao risco de "colagem" da identidade do dono do chip

ao uso de todos no aparelho. Em outras palavras: Uma criança poderá usar o celular da mãe e acessar conteúdos inadequados.

9. **"Graph social" e sinais de terceiros sem consentimento explícito**
    - **Porquê não:** aqui se refere ao uso da rede de conexões de uma pessoa (amigos, seguidores, contatos) e das interações com esses terceiros para tentar inferir sua idade. Em outras palavras, em vez de perguntar diretamente a idade do usuário, o sistema olha para quem ele segue, quais conteúdos consome, em que grupos participa e, a partir desse "grafo social", estima se ele é menor ou maior de idade. Possui alto risco para privacidade e transparência; além de decisões opacas.

10. **Gate único na app store como "bala de prata"**

- **Porquê não:** não cobre acesso via web; concentra poder em poucas empresas; cria custos de migração e adaptação para todo o ecossistema. O debate internacional tem sido "qual camada" e "em que momento", não "uma única porta".

4) O que QUEREMOS

Este bloco junta padrões regulatórios modernos e caminhos concretos de implementação.

4.1 Sete requisitos funcionais traduzidos em engenharia

1. **Resistência contra fraude:** o sistema precisa ser robusto contra tentativas de enganar. Modelos de biometria facial podem ser driblados com fotos ou vídeos falsos. Já o uso de CPF abre risco de tráfico de documentos. A solução mais segura é trabalhar com tokens temporários, emitidos por terceiros confiáveis, que expiram rapidamente e não podem ser reutilizados. Esse modelo segue referências internacionais como o DSA europeu e o guia técnico da Arcom francesa[13] [14].

2. **Apenas a informação se é ou não maior de 18 anos, nem a idade, nem a identidade:** o site que recebe o usuário não deve ter acesso a dados pessoais, apenas à informação "maior de 18 anos". Nem nome, nem CPF, nem data de nascimento. Além disso, o verificador não sabe em qual site a pessoa entrou. Esse princípio de "dupla confidencialidade" já está formalizado na França e garante proteção da identidade e da privacidade desde a concepção do sistema[15].

---

[13] ARCOM. Référentiel technique sur la vérification de l'âge. Paris: Autorité de régulation de la communication audiovisuelle et numérique, 2024. Disponível em: https://www.arcom.fr/. Acesso em: 23 set. 2025.

[14] COMISSÃO EUROPEIA. Diretrizes para o Artigo 28 do Digital Services Act: proteção de menores e verificação etária. Bruxelas: European Commission, 2025. Disponível em: https://digital-strategy.ec.europa.eu/. Acesso em: 23 set. 2025.

[15] ARCOM. Référentiel technique sur la vérification de l'âge. Paris: Autorité de régulation de la communication audiovisuelle et numérique, 2024. Disponível em: https://www.arcom.fr/. Acesso em: 23 set. 2025.

3. **Dupla confidencialidade (double blind):** o sistema deve garantir que nenhuma das partes veja mais do que o necessário. O site acessado só recebe a informação de que o usuário é maior de 18 anos, sem saber sua identidade. O verificador de idade, por sua vez, não sabe em qual site a pessoa entrou. Esse arranjo impede o cruzamento de dados entre serviços, reduz risco de rastreamento e preserva a privacidade por design.

4. **Auditar o processo, não o usuário:** é fundamental registrar e guardar provas de que o sistema de verificação funciona corretamente. Esses logs devem mostrar se a solução é segura, atualizada e em conformidade com os padrões técnicos. Porém, nunca podem rastrear o que cada pessoa acessa ou faz. A auditoria é sobre o mecanismo, não sobre o indivíduo, seguindo as diretrizes do DSA para proporcionalidade e minimização[16].

5. **Controle de validade (reemitir e revogar quando preciso):** o sistema precisa ter mecanismos para renovar ou cancelar tokens, mantendo um histórico de conformidade. Isso evita que usuários burlem o processo criando várias contas. A autoridade australiana recomenda controles proativos de detecção[17] [18].

6. **Verificação online sem guardar documentos:** não é seguro pedir upload permanente de documentos. A verificação deve gerar apenas um token reutilizável, que funcione em diferentes serviços. Experiências como o euCONSENT na Europa e o demonstrador da CNIL mostram como esse modelo protege a privacidade[19] [20].

7. **Sistema justo e acessível para todos:** a verificação não pode excluir quem não tem cartão de crédito, documento atualizado ou celular moderno. É essencial oferecer opções alternativas com igual confiança, reduzir barreiras socioeconômicas e prever acessibilidade de idioma e tecnologia. O DSA europeu reforça a necessidade de proporcionalidade e não discriminação[21] [22].

---

[16] COMISSÃO EUROPEIA. Diretrizes para o Artigo 28 do Digital Services Act: proteção de menores e verificação etária. Bruxelas: European Commission, 2025. Disponível em: https://digital-strategy.ec.europa.eu/. Acesso em: 23 set. 2025.

[17] ESAFETY COMMISSIONER. Roadmap for age verification. Canberra: eSafety, 2023. Disponível em: https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf. Acesso em: 23 set. 2025.

[18] ESAFETY COMMISSIONER. Behind the screen: transparency report. Canberra: eSafety, 2025. Disponível em: https://www.esafety.gov.au/about-us/research. Acesso em: 23 set. 2025.

[19] ESAFETY COMMISSIONER. Roadmap for age verification. Canberra: eSafety, 2023. Disponível em: https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf. Acesso em: 23 set. 2025.

[20] ESAFETY COMMISSIONER. Behind the screen: transparency report. Canberra: eSafety, 2025. Disponível em: https://www.esafety.gov.au/about-us/research. Acesso em: 23 set. 2025.

[21] ESAFETY COMMISSIONER. Roadmap for age verification. Canberra: eSafety, 2023. Disponível em: https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf. Acesso em: 23 set. 2025.

[22] ESAFETY COMMISSIONER. Behind the screen: transparency report. Canberra: eSafety, 2025. Disponível em: https://www.esafety.gov.au/about-us/research. Acesso em: 23 set. 2025.

4.2 Caminhos tecnológicos complementares

A) "GovBR com privacidade"

- O GovBR é alternativa válida como emissor de atributos, mas hoje não é privativo o suficiente para prova de idade reutilizável sem exposição. Precisaria evoluir para credenciais verificáveis com prova de atributo (18+) via Zero Knowledge Protocol (ZKP) "prova de conhecimento zero", emissão de tokens efêmeros e separação rígida entre emissor e verificador. Isso exige fortalecimento de capacidades estatais e amadurecimento do ecossistema de identidade soberana.

- Alternativa de transição temporária: instituições técnicas independentes, como o NIC.br, poderiam atuar como entidade neutra de confiança pública, responsável por intermediar a emissão e validação de atributos até que o GovBR evolua para um modelo plenamente privativo. Essa função temporária garantiria interoperabilidade, transparência e auditoria, sem concentrar poder excessivo em um único emissor. Na prática: GovBR → continua sendo a fonte oficial do dado (quem tem condições de atestar a identidade e a idade da pessoa). NIC.br → age como camada de privacidade: recebe a resposta do GovBR, aplica o filtro de atributo (só "+18" ou "não"), emite o token efêmero. Site → só recebe o resultado binário (sim/não), sem nunca ver o CPF, data de nascimento ou outros dados. Ou seja, é o NIC.br que garante o **"double blind":** o site não sabe quem é o usuário, e o GovBR não sabe em qual site a prova foi usada.

B) Ecossistema de certificados digitais interoperáveis

- **Usar padrões abertos (W3C Verifiable Credentials, SD-JWT, ZKPs)**, verificadores independentes certificados, e integração por APIs. Europa está financiando uma "solução europeia de verificação da idade" interoperável e referência.

4.3 Proporcionalidade e foco em risco

- Distinguir claramente **onde verificação forte é necessária:** conteúdo adulto sexual, jogos de azar, venda de álcool, acompanhantes etc. E **onde não é:** jornalismo, esportes, conhecimento, comércio sem conteúdo adulto. Esse recorte ecoa padrões internacionais.

- O objetivo é impedir acesso indevido a conteúdos 18+ e reduzir riscos **sem bloquear conhecimento, jornalismo e demais**. Redes de tokens por atributo, dupla confidencialidade e proporcionalidade evitam o erro de "age-gate cego" em informação pública.